

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-169726

(43)Date of publication of application : 14.06.2002

-----  
-----  
(51)Int.Cl. G06F 12/14

G09C 1/00

H04L 9/08

-----  
-----  
(21)Application number : 2000-364896 (71)Applicant : SONY CORP

(22)Date of filing : 30.11.2000 (72)Inventor : SANETO TAKANORI  
KAWAKAMI TATSU  
KITATANI YOSHIMICHI

-----  
-----  
(54) DEVICE AND METHOD FOR INFORMATION PROCESSING AND PROGRAM  
STORAGE MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To use contents by a desired information processor while preventing a third party who has no proper right from using.

SOLUTION: An authenticating server 3 receives data specifying a contents managing program sent from a personal computer 1-1, generates a group key to be used by a group in common, records the data specifying the contents managing program and group key while making them correspond to each other, and sends the group key to the personal computer 1-1.

**\* NOTICES \***

JPO and INPIT are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.\*\*\*\* shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

---

**CLAIMS**

---

[Claim(s)]

[Claim 1]An information processor comprising:

The 1st reception means that receives identification data transmitted from other information processors.

A creating means which generates a group key shared in a group to whom an information processor besides the above belongs when said identification data is received.

A recording device which records said group key corresponding to said identification data.

The 1st transmitting means that transmits said group key to an information processor besides the above.

[Claim 2]said 1st reception means -- as said identification data -- said -- others -- the information processor according to claim 1 receiving data which specifies a program for contents managing of an information processor.

[Claim 3]The information processor according to claim 1 when said 1st reception means receives said creating means said identification data for the first time from an information processor besides the same group's above, wherein ID which specifies said group also generates further.

[Claim 4]An information processing method comprising:

A receiving step which receives identification data transmitted from an information processor.

A generation step which generates a group key shared in a group to whom said information processor belongs when said identification data is received.

A record step which records said group key corresponding to said identification data.

A transmission step which transmits said group key to said information processor.

[Claim 5]A program storing medium with which a program which a computer can read is stored, comprising:

A receiving step which receives identification data transmitted from an information processor.

A generation step which generates a group key shared in a group to whom said information processor belongs when said identification data is received.

A record step which records said group key corresponding to said identification data.

A transmission step which transmits said group key to said information processor.

[Claim 6]An information processor which manages copy operation of information by an information processor besides the above based on a group key which two or more of other information processors have, and which is shared in a group, comprising:

A memory measure which memorizes ID which specifies said group.

A reception means which receives ID which specifies said group from an information processor besides the above.

Said ID memorized by said memory measure.

A comparison means to compare said ID received by said reception means.

An output means which outputs data which recognizes copy operation of the information to an information processor besides the above based on a comparison result of said comparison means.

[Claim 7]The information processor according to claim 6, wherein said memory measure memorizes a password further, said reception means receives said password further and said comparison means compares said ID with a password.

[Claim 8]An information processing method which manages copy operation of information by said information processor based on a group key which two or more information processors have, and which is shared in a group, comprising:

A memory step which memorizes ID which specifies said group.

A receiving step which receives ID which specifies said group from said information processor.

Said ID memorized by processing of said memory step.

A comparison step which compares said ID received by processing of said receiving step.

An output step which outputs data which recognizes copy operation of the information to said information processor based on a comparison result of processing of said comparison step.

[Claim 9]Based on a group key which two or more information processors have and which is shared in a group, A memory step which memorizes ID which is a program for information processing which manages copy operation of information by said

information processor, and specifies said group, A receiving step which receives ID which specifies said group from said information processor, A comparison step which compares said ID memorized by processing of said memory step with said ID received by processing of said receiving step, A program storing medium with which a program which a computer by which an output step which outputs data which recognizes copy operation of the information being included to said information processor based on a comparison result of processing of said comparison step can read is stored.

[Claim 10]An information processor comprising:

The 1st transmitting means that transmits identification data to other 1st information processor.

The 1st reception means that receives a group key shared in a group from said other 1st information processor.

A memory measure which memorizes said group key received by said 1st reception means.

An encoding means which enciphers a contents key which has enciphered said contents with said group key when outputting contents.

[Claim 11]The information processor according to claim 10, wherein said encoding means enciphers said contents key decoded by said decoding means, including further a decoding means which decodes said contents key.

[Claim 12]ID which specifies said group, an acquisition means which acquires a password, and said ID acquired by said acquisition means and the 2nd transmitting means that transmits a password to other 2nd information processor, The 2nd reception means that receives data which recognizes copy operation of said contents from said other 2nd information processor, The information processor according to claim 10 by which a copy control means to control copy operation of said contents being further included based on data which recognizes copy operation of said contents received by said 2nd reception means.

[Claim 13]The information processor according to claim 10, wherein said 1st transmitting means transmits data which specifies a program for contents managing of said information processor as said identification data.

[Claim 14]An information processing method comprising:

A transmission step which transmits identification data to an information processor.

A receiving step which receives a group key shared in a group from said information processor.

A memory step which memorizes said group key received by processing of said receiving step.

An encryption step which enciphers a contents key which has enciphered said contents with said group key when outputting contents.

[Claim 15]A program storing medium with which a program which a computer can read is stored, comprising:

A transmission step which transmits identification data to an information processor.

A receiving step which receives a group key shared in a group from said information processor.

A memory step which memorizes said group key received by processing of said receiving step.

An encryption step which enciphers a contents key which has enciphered said contents with said group key when outputting contents.

---

## DETAILED DESCRIPTION

---

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention relates to the information processor which prevents use of inaccurate contents especially, a method, and a program storing medium about an information processor, a method, and a program storing medium.

[0002]

[Description of the Prior Art]The art of preventing unjust use of contents is used by enciphering contents, such as music and a picture.

[0003]Drawing 1 is a figure explaining the program decoded when enciphering and recording the conventional contents and reproducing. Based on ID and the password which were entered by the user, a secrecy program generates an enciphering key and enciphers contents with the generated enciphering key.

[0004]When it is enciphered and contents are reproduced, a decipherment program requires the input of ID and a password of a user, when right ID and a password are entered, a decode key is generated based on ID and a password, and contents are decoded with a decode key.

[0005]By doing in this way, if right ID and a password are not known, contents cannot be used but unjust use of contents can be prevented.

[0006]A decode key is enciphered with a storage key and the art of making secure one memorizing a storage key is also used for the apparatus using contents.

[0007]

[Problem(s) to be Solved by the Invention]However, the user who owns two or more apparatus when using contents by the apparatus which enciphered the decode key with the storage key and has memorized the storage key to secure one, Predetermined contents could be used only by predetermined apparatus and there was a problem that desired contents could not be used by desired apparatus.

[0008]This invention is made in view of such a situation, and it aims at enabling it to use desired contents by desired apparatus, preventing use of the third party who does not have a just right.

[0009]

[Means for Solving the Problem]written this invention is characterized by it having been alike and comprising the following at claim 1.

The 1st reception means that receives identification data transmitted from other information processors.

A creating means which generates a group key shared in a group to whom other information processors belong when identification data is received.

A recording device which records a group key corresponding to identification data.

The 1st transmitting means that transmits a group key to other information processors.

[0010]The 1st reception means can receive data which specifies a program for contents managing of other information processors as identification data.

[0011]The creating means can also generate further ID which specifies a group, when the 1st reception means receives identification data for the first time from other information processors of the same group.

[0012]written this invention is characterized by it having been alike and comprising the following at claim 4.

A receiving step which receives identification data transmitted from an information processor.

A generation step which generates a group key shared in a group to whom an information processor belongs when identification data is received.

A record step which records a group key corresponding to identification data.

A transmission step which transmits a group key to an information processor.

[0013]Written this invention is characterized by a program of a storing medium comprising the following at claim 5.

A receiving step which receives identification data transmitted from an information processor.

A generation step which generates a group key shared in a group to whom an information processor belongs when identification data is received.

A record step which records a group key corresponding to identification data.

A transmission step which transmits a group key to an information processor.

[0014]A memory measure the information processor according to claim 6 remembers ID which specifies a group to be, A reception means which receives ID which specifies a group from other information processors, A comparison means to compare ID

memorized by a memory measure with ID received by a reception means, and an output means which outputs data which recognizes copy operation of the information to other information processors based on a comparison result of a comparison means are included.

[0015]A memory measure memorizes a password further, a reception means receives a password further, and the comparison means can compare ID with a password.

[0016]A memory step the information processing method according to claim 8 remembers ID which specifies a group to be, A receiving step which receives ID which specifies a group from an information processor, A comparison step which compares ID memorized by processing of a memory step with ID received by processing of a receiving step, Based on a comparison result of processing of a comparison step, an output step which outputs data which recognizes copy operation of the information is included to an information processor.

[0017]A program of the program storing medium according to claim 9, A memory step which memorizes ID which specifies a group, and a receiving step which receives ID which specifies a group from an information processor, A comparison step which compares ID memorized by processing of a memory step with ID received by processing of a receiving step, Based on a comparison result of processing of a comparison step, an output step which outputs data which recognizes copy operation of the information is included to an information processor.

[0018]written this invention is characterized by it having been alike and comprising the following at claim 10.

The 1st transmitting means that transmits identification data to other 1st information processor.

The 1st reception means that receives a group key shared in a group from other 1st information processor.

A memory measure which memorizes a group key received by the 1st reception means.

An encoding means which enciphers a contents key which has enciphered contents with a group key when outputting contents.

[0019]An information processor establishes further a decoding means which decodes a contents key, and the encoding means can encipher a contents key decoded by decoding means.

[0020]ID as which an information processor specifies a group, and an acquisition means which acquires a password, ID acquired by acquisition means and the 2nd transmitting means that transmits a password to other 2nd information processor, The 2nd reception means that receives data which recognizes copy operation of contents from other 2nd information processor, and a copy control means to control copy operation of contents based on data which recognizes copy operation of

contents received by the 2nd reception means can be formed further.

[0021]The 1st transmitting means can transmit data which specifies a program for contents managing of an information processor as identification data.

[0022]written this invention is characterized by it having been alike and comprising the following at claim 14.

A transmission step which transmits identification data to an information processor.

A receiving step which receives a group key shared in a group from an information processor.

A memory step which memorizes a group key received by processing of a receiving step.

An encryption step which enciphers a contents key which has enciphered contents with a group key when outputting contents.

[0023]Written this invention is characterized by a program of a storing medium comprising the following at claim 15.

A transmission step which transmits identification data to an information processor.

A receiving step which receives a group key shared in a group from an information processor.

A memory step which memorizes a group key received by processing of a receiving step.

An encryption step which enciphers a contents key which has enciphered contents with a group key when outputting contents.

[0024]In the information processor according to claim 1, the information processing method according to claim 4, and the program storing medium according to claim 5, When identification data transmitted from other information processors is received and identification data is received, a group key shared in a group to whom other information processors belong is generated, a group key is recorded corresponding to identification data, and a group key is transmitted to other information processors.

[0025]In the information processor according to claim 6, the information processing method according to claim 8, and the program storing medium according to claim 9, ID which specifies a group is memorized, ID which specifies a group from other information processors is received, ID memorized is compared with received ID, and data which recognizes copy operation of the information is outputted to other information processors based on a comparison result.

[0026]In the information processor according to claim 10, the information processing method according to claim 14, and the program storing medium according to claim 15, To other 1st information processor, identification data is transmitted and from other 1st information processor. When a group key shared in a group is received, a received group key is memorized and it outputs contents, a contents key which has enciphered



contents is enciphered with a group key.

[0027]

[Embodiment of the Invention]Drawing 2 is a figure showing the 1 embodiment of the music data managerial system concerning this invention. The personal computer 1-1 is connected to the network 2 which comprises a Local Area Network or the Internet.

[0028]The personal computer 1-1 performs the contents managing program 51, the display operation instruction program 52 and the application program 54-1 for purchase thru/or 54-3, and it constitutes the contents database 53 in the inside.

[0029]Although the contents managing program 51 is mentioned later for details, encipher contents, and it is made to record on the contents database 53, and it manages use of the contents which are enciphered and are recorded on the contents database 53.

[0030]The display operation instruction program 52 gives directions of the directions corresponding to operation in which it was inputted, for example, reproduction of contents, import of contents, etc. to the contents managing program 51 while displaying the information related to contents.

[0031]The contents database 53 records the contents which were supplied from the contents managing program 51 and which are enciphered, and it supplies the contents enciphered corresponding to the demand of the contents managing program 51 to the contents managing program 51.

[0032]The application program 54-1 for purchase thru/or 54-3 perform processing of the purchase of EMD server 4-1 thru/or the contents from 4-3. The application program 54-1 for purchase thru/or 54-3 are combined with the contents managing program 51 by SAC (Secure Authentication Channel).

[0033]The application program 54-3 for purchase executes the group gateway programs 61. It enciphers with the group key which mentions the contents key for decoding contents later, and the group gateway programs 61 enable it to use contents only by the apparatus permitted, when outputting the contents enciphered outside. The group gateway programs 61 are decoded with the group key which mentions the contents key for decoding contents later, when importing the contents enciphered. Import means recording contents in the available state.

[0034]Via the network 2, the personal computer 1-1 and the personal computer 1-2 transmit the number of a user's credit card to the recognition server 3, register it into the recognition server 3, and acquire the group key later mentioned from the recognition server 3, ID, and a password.

[0035]The recognition server 3 makes the number of the credit card of the user of the personal computer 1-1, ID, and a password record on the ID management server 8, when the personal computer 1-1 is registered. The recognition server 3 recognizes the personal computer 1-2, when the personal computer 1-2, for example, imports the contents outputted from the personal computer 1-1.

[0036]The personal computer 1-2 cannot import the contents outputted from the personal computer 1-1, when not recognized from the recognition server 3.

[0037]. Received the personal computer 1-1 from the EMD (Electrical Music Distribution) server 4-1 thru/or 4-3. Or the data of the music read in CD (Compact Disc) mentioned later. While changing into the method (for example, ATRAC3 (trademark)) of predetermined compression of (contents are called hereafter), it enciphers and records with cipher systems, such as DES (Data Encryption Standard).

[0038]The personal computer 1-1 records the data of a utilization condition in which the utilization condition of contents is shown corresponding to the contents currently enciphered and recorded. . The data of a utilization condition can use simultaneously the contents corresponding to the data of the utilization condition by three sets (Portable Device (it is also called PD)) of the portable devices 12-1, and 12-3, for example. It is shown that it can copy, that it can move to other personal computers, etc.

[0039]The contents which encipher the personal computer 1-1 and are recorded with the data (for example, a track name, reproduction frequency, a reproduction term, or equalizer information etc.) relevant to contents. While making the portable device 12-1 connected memorize, corresponding to having made the portable device 12-1 memorize, the data of the utilization condition corresponding to the contents made to memorize is updated (check-out is called hereafter). The contents which encipher the personal computer 1-1 and are recorded with the data relevant to contents. While making the portable device 12-2 connected memorize, corresponding to having made the portable device 12-2 memorize, the data of the utilization condition corresponding to the contents made to memorize is updated. The contents which encipher the personal computer 1-1 and are recorded with the data relevant to contents. While making the portable device 12-3 connected memorize, corresponding to having made the portable device 12-3 memorize, the data of the utilization condition corresponding to the contents made to memorize is updated.

[0040]The contents which the personal computer 1-1 checked out to the portable device 12-1 which is connected as for the personal computer 1-1, The data of the utilization condition corresponding to the contents which made the portable device 12-1 eliminate, and were made to eliminate is updated (check-in is called hereafter). The personal computer 1-1 updates the data of the utilization condition corresponding to the contents which made the portable device 12-2 eliminate the contents which the personal computer 1-1 checked out to the portable device 12-2 connected, and made it eliminate them. The personal computer 1-1 updates the data of the utilization condition corresponding to the contents which made the portable device 12-3 eliminate the contents which the personal computer 1-1 checked out to the portable device 12-3 connected, and made it eliminate them.

[0041]The personal computer 1-1 cannot check in at the contents which the personal

computer 1-2 checked out to the portable device 12-1. The personal computer 1-1 cannot check in at the contents which the personal computer 1-2 checked out to the portable device 12-2. The personal computer 1-1 cannot check in at the contents which the personal computer 1-2 checked out to the portable device 12-3.

[0042]The personal computer 1-2 is connected to the network 2 which comprises a Local Area Network or the Internet. With cipher systems, such as DES, it enciphers and the personal computer 1-2 records them while changing into the method of predetermined compression the contents read in CD which was received from EMD server 4-1 thru/or 4-3, or is mentioned later.

[0043]The personal computer 1-2 records the data of a utilization condition in which the utilization condition of contents is shown corresponding to the contents currently enciphered and recorded. It is shown that the contents corresponding to the data of the utilization condition can be copied [ which can be simultaneously used by three sets of portable devices ] for example, that the data of a utilization condition is movable to other personal computers, etc.

[0044]The contents which encipher the personal computer 1-2 and are recorded with the data relevant to contents. While making the portable device 12-4 connected memorize, corresponding to having made the portable device 12-4 memorize, the data of the utilization condition corresponding to the contents made to memorize is updated (that is, he checks out). When there are directions of check-out of contents, the personal computer 1-2 does not check out the contents to the portable device 12-4, when the expiration date or reproduction frequency later mentioned to the contents is set up.

[0045]The personal computer 1-2 updates the data of the utilization condition corresponding to the contents which made the portable device 12-4 eliminate the contents which the personal computer 1-2 checked out to the portable device 12-4 connected, and made it eliminate them.

[0046]The personal computer 1-2 cannot check in at the contents which the personal computer 1-1 checked out to the portable device 12-4.

[0047]Hereafter, when it is not necessary to distinguish the personal computer 1-1 and the personal computer 1-2 separately, the personal computer 1 is only called.

[0048]EMD server 4-1 supplies contents to the personal computer 1 with the data relevant to contents via the network 2 corresponding to the demand of the personal computer 1. EMD server 4-2 supplies contents to the personal computer 1 with the data relevant to contents via the network 2 corresponding to the demand of the personal computer 1.

[0049]Corresponding to the demand of the personal computer 1, EMD server 4-3 via the network 2 with the data (for example, a track name, reproduction frequency, a reproduction term, or equalizer information etc.) relevant to contents. The contents supplied from the EMD contents database 5 or the contents supplied from the rise low

DETTO contents database 6 are supplied to the personal computer 1. EMD server 4-1 supplies the data for an advertisement supplied from the advertisement system 7 via the network 2 to the personal computer 1-1 or the personal computer 1-2.

[0050]The contents which EMD server 4-1 thru/or each of 4-3 supply are compressed by the method of the same or different compression. The contents which EMD server 4-1 thru/or each of 4-3 supply are enciphered by the method of the same or different encryption.

[0051]When a user purchases contents from EMD server 4-1 thru/or either of 4-5, the ID management server 8, By registration of the personal computer 1-1, the number of the credit card of the user of the recorded personal computer 1-1, ID, and a password are transmitted to EMD server 4-1 with which contents are purchased thru/or either of 4-5. EMD server 4-1 thru/or 4-5 perform processing of fee collection based on the number of the credit card supplied from the ID management server 8, ID, and a password, when contents are sold.

[0052]As for the group manager system 9, record or transmission of registration of the recognition server 3 or recognition of use of contents and the number of the credit card of the ID management server 8, ID, and a password, etc. manages contents, ID, the utilization condition of a password, etc.

[0053]The locker server 11 records the contents supplied from the personal computer 1-1 or the personal computer 1-2 via the network 2, and caters to the Request to Send of contents, The contents currently recorded are transmitted to the personal computer 1-1 or the personal computer 1-2.

[0054]Contents (.) to which the portable device 12-1 was supplied from the personal computer 1 Namely, the checked-out contents are stored in the memory card 13-1 with which it is equipped with the data (for example, a track name, reproduction frequency, a reproduction term, or equalizer information etc.) relevant to contents. Based on the data relevant to contents, the portable device 12-1 is reproduced and outputs the contents memorized to the memory card 13-1 to the beef fat phone etc. which are not illustrated.

[0055]For example, when it is going to reproduce exceeding the reproduction frequency memorized as data relevant to contents, the portable device 12-1 suspends reproduction of corresponding contents. When it is going to reproduce after passing over the reproduction term memorized as data relevant to contents, the portable device 12-1 suspends reproduction of corresponding contents. The portable device 12-1 equalizes and outputs a sound based on the equalizer information memorized as data relevant to contents.

[0056]The user can remove and walk around with the portable device 12-1 from the personal computer 1, can reproduce the contents memorized to the memory card 13-1, and can listen to the music corresponding to contents, etc. by headphone etc.

[0057]The portable device 12-1 can reproduce the contents memorized by the

memory card 13-2 by equipping with the memory card 13-2 which has memorized the contents supplied by the terminal unit 14 currently installed in the shop front etc.

[0058]The memory card 13-1 in which contents were memorized via the portable device 12-1 is removed from the portable device 12-1, and the music center of the car 15 is equipped with it. The music center of the car 15 by which it was equipped with the memory card 13-1 reads the contents memorized by the memory card 13-1, and reproduces contents.

[0059]Via the network 2, the digital cellular phone terminal 16 with a camera with which it is equipped with the memory card 13-3 requires supply of contents of EMD server 4-4, and stores in the memory card 13-3 the contents supplied from EMD server 4-4. The digital cellular phone terminal 16 with a camera reproduces the contents memorized by the memory card 13-3 with which it is equipped. The portable device 12-1 can reproduce the contents memorized by the memory card 13-3 by equipping with the memory card 13-3 which has memorized contents.

[0060]The portable device 12-2 memorizes the contents supplied from the personal computer 1 with the data relevant to contents. Based on the data relevant to contents, the portable device 12-2 is reproduced and outputs the memorized contents to the beef fat phone etc. which are not illustrated. The user can reproduce the memorized contents with which removed the portable device 12-2 which memorized contents from the personal computer 1, and it walked around, and can listen to the music corresponding to contents, etc. by headphone etc.

[0061]The portable device 12-3 memorizes the contents supplied from the personal computer 1 with the data relevant to contents. Based on the data relevant to contents, the portable device 12-3 is reproduced and outputs the memorized contents to the beef fat phone etc. which are not illustrated. The user can reproduce the memorized contents with which removed the portable device 12-3 which memorized contents from the personal computer 1, and it walked around, and can listen to the music corresponding to contents, etc. by headphone etc.

[0062]The portable device 12-4 memorizes the contents (it restricts to the contents to which the expiration date or reproduction frequency mentioned later is not set) supplied from the personal computer 1 with the data relevant to contents. Based on the data relevant to contents, the portable device 12-4 is reproduced and outputs the memorized contents to the beef fat phone etc. which are not illustrated. The user can reproduce the memorized contents with which removed the portable device 12-4 which memorized contents from the personal computer 1, and it walked around, and can listen to the music corresponding to contents, etc. by headphone etc.

[0063]Via the network 2, the home music center 17 requires supply of contents of EMD server 4-5, memorizes the contents supplied from EMD server 4-5, and reproduces the memorized contents.

[0064]Drawing 3 is a figure explaining the composition of the personal computer 1-1.

CPU(Central Processing Unit) 71 actually performs application programs, such as the contents managing program 51 or the group gateway programs 61, and OS (Operating System). Generally, ROM(Read-onlyMemory) 72 stores fixed data fundamentally of the parameters the program which CPU71 uses, and for an operation. In the program used in execution of CPU71, and its execution, RAM(Random-Access Memory) 73 stores a variable parameter suitably. These are mutually connected by the host bus 74 which comprises a CPU bus etc.

[0065]The host bus 74 is connected to the external buses 76, such as a PCI (Peripheral ComponentInterconnect/Interface) bus, via the bridge 75.

[0066]The keyboard 78 is operated by the user when inputting various kinds of instructions into CPU71. The mouse 79 is operated by the user when performing the directions and selection of the point on the screen of the display 80. The display 80 comprises a liquid crystal display or CRT (Cathode Ray Tube), and displays a variety of information in a text or an image. HDD(Hard Disk Drive) 81 drives a hard disk, and records or reproduces the program and information which are performed by CPU71 to them.

[0067]The drive 82 reads the data or the program currently recorded on the magnetic disk 91 with which it is equipped, the optical disc 92 (CD is included), the magneto-optical disc 93, or the semiconductor memory 94, The data or program is supplied to RAM73 connected via the interface 77, the external bus 76, the bridge 75, and the host bus 74.

[0068]The portable device 12-1 is connected to the USB (Universal Serial Bus) port 83-1 via a predetermined cable. USB port 83-1 via the interface 77, the external bus 76, the bridge 75, or the host bus 74, HDD81, CPU71, or the data (for example, the command of contents or the portable device 12-1, etc. are included) supplied from RAM73 is outputted to the portable device 12-1.

[0069]The portable device 12-2 is connected to USB port 83-2 via a predetermined cable. USB port 83-2 via the interface 77, the external bus 76, the bridge 75, or the host bus 74, HDD81, CPU71, or the data (for example, the command of contents or the portable device 12-2, etc. are included) supplied from RAM73 is outputted to the portable device 12-2.

[0070]The portable device 12-3 is connected to USB port 83-3 via a predetermined cable. USB port 83-3 via the interface 77, the external bus 76, the bridge 75, or the host bus 74, HDD81, CPU71, or the data (for example, the command of contents or the portable device 12-3, etc. are included) supplied from RAM73 is outputted to the portable device 12-3.

[0071]The loudspeaker 24 outputs the predetermined sound corresponding to contents the data supplied from the interface 77, or based on an audio signal.

[0072]These keyboards 78 thru/or loudspeakers 84 is connected to the interface 77, and the interface 77 is connected to CPU71 via the external bus 76, the bridge 75, and

the host bus 74.

[0073]The network 2 is connected and the communications department 85 stores in the packet of a prescribed method the data (for example, the demand of registration or the Request to Send of contents etc.) supplied from CPU71 or HDD81, While transmitting via the network 2, the data (for example, an authentication key, contents, etc.) stored in the packet which received is outputted to CPU71, RAM73, or HDD81 via the network 2.

[0074]The communications department 85 is connected to CPU71 via the external bus 76, the bridge 75, and the host bus 74.

[0075]Since the composition of the personal computer 1-2 is the same as the composition of the personal computer 1-1, the explanation is omitted.

[0076]Drawing 4 is a figure explaining the composition of the recognition server 3. CPU101 actually performs application programs, such as a Web server program, and OS. Generally, ROM102 stores fixed data fundamentally of the parameters the program which CPU101 uses, and for an operation. In the program used in execution of CPU101, and its execution, RAM103 stores a variable parameter suitably. These are mutually connected by the host bus 104 which comprises a CPU bus etc.

[0077]The host bus 104 is connected to the external buses 106, such as a PCI bus, via the bridge 105.

[0078]The keyboard 108 is operated by the user when inputting various kinds of instructions into CPU101. The mouse 109 is operated by the user when performing the directions and selection of the point on the screen of the display 110. The display 110 comprises a liquid crystal display or CRT, and displays a variety of information in a text or an image. HDD111 drives a hard disk, and records or reproduces the program and information which are performed by CPU101 to them.

[0079]The drive 112 reads the data or the program currently recorded on the magnetic disk 131 with which it is equipped, the optical disc 132, the magneto-optical disc 133, or the semiconductor memory 134, The data or program is supplied to RAM103 connected via the interface 107, the external bus 106, the bridge 105, and the host bus 104.

[0080]These keyboards 108 thru/or drives 112 is connected to the interface 107, and the interface 107 is connected to CPU101 via the external bus 106, the bridge 105, and the host bus 104.

[0081]The network 2 is connected and the communications department 113 via the network 2, While outputting the data (for example, data required for the registration mentioned later or ID (Identifier) of a predetermined program etc.) stored in the packet which received to CPU101, RAM103, or HDD111, The data (for example, ID or a password etc.) supplied from CPU101 or HDD111 is stored in the packet of a prescribed method, and it transmits via the network 2.

[0082]The communications department 113 is connected to CPU101 via the external

bus 106, the bridge 105, and the host bus 104.

[0083]Since each composition of EMD server 4-1 thru/or 4-5, the ID management server 8, and the locker server 11 is the same as the composition of the recognition server 3, the explanation is omitted.

[0084]Next, the function realized when the personal computer 1-1 executes a predetermined program is explained.

[0085]Drawing 5 is a block diagram explaining the composition of the function of the personal computer 1-1 realized by execution of the predetermined program of CPU71, etc.

[0086]The contents managing program 51, The EMD selection program 171, check-in / checkout control program 172, the cipher system conversion program 173, the compression technology conversion program 174, the enciphered program 175, the utilization condition conversion program 176, the signature control program 177, the authentication program 178, It comprises two or more programs, such as the decoding program 179 and the driver 180 for PD.

[0087]The instruction by which the contents managing program 51 is shuffled, for example, or it is described by the instruction etc. which are enciphered, the contents of processing are concealed from the outside, and reading comprehension of the contents of processing becomes difficult (for example, a user cannot specify an instruction, even if it reads the contents managing program 51 directly) -- it is constituted like.

[0088]When the contents managing program 51 is installed in the personal computer 1, the EMD selection program 171 is not contained in the contents managing program 51, but is received from the registration server which is not illustrated via the network 2 in processing of registration of EMD. The EMD selection program 171 chooses connection with EMD server 4-1 thru/or either of 4-3, The application 54-1 for purchase thru/or 54-3 are made to perform communications (for example, download of contents when purchasing contents, etc.) with EMD server 4-1 thru/or either of 4-3.

[0089]Check-in / checkout control program 172, Based on the utilization condition file 202-1 thru/or 202-N currently recorded on check-in or setting out of check-out, and the contents database 53, He checks in at the contents which check out the contents stored in the contents file 201-1 thru/or 201-N to the portable device 12-1 thru/or either of 12-3, or are memorized by the portable device 12-1 thru/or 12-3.

[0090]Check-in / checkout control program 172 updates the data of the utilization condition stored in the utilization condition file 202-1 thru/or 202-N currently recorded on the contents database 53 corresponding to processing of check-in or check-out.

[0091]The method of encryption of contents with which the application program 54-1 for purchase received the cipher system conversion program 173 from EMD server



4-1 via the network 2, The method of encryption of the contents which the application program 54-2 for purchase received from EMD server 4-2, Or the method of encryption of the contents which the application program 54-3 for purchase received from EMD server 4-3 is transformed into the method of the same encryption as the contents stored in the contents file 201-1 thru/or 201-N which the contents database 53 is recording.

[0092]The cipher system conversion program 173 changes the contents to check out into the portable device 12-1 or a cipher system with available 12-3, when you check out contents to the portable device 12-1 or 12-3.

[0093]The method of compression of contents with which the application program 54-1 for purchase received the compression technology conversion program 174 from EMD server 4-1 via the network 2, The method of compression of the contents which the application program 54-2 for purchase received from EMD server 4-2, Or the method of compression of the contents which the application program 54-3 for purchase received from EMD server 4-3 is transformed into the method of the same compression as the contents stored in the contents file 201-1 thru/or 201-N which the contents database 53 is recording.

[0094]The contents (not compressed) which the compression technology conversion program 174 was read in CD, for example, and were supplied from the sound recording program 151, It codes by the method of the same coding as the contents stored in the contents file 201-1 thru/or 201-N which the contents database 53 is recording.

[0095]The compression technology conversion program 174 changes the contents to check out into the portable device 12-1 or the method of compression with available 12-3, when you check out contents to the portable device 12-1 or 12-3.

[0096]The contents (not enciphered) which the enciphered program 175 was read in CD, for example, and were supplied from the sound recording program 151, It enciphers by the method of the same encryption as the contents stored in the contents file 201-1 thru/or 201-N which the contents database 53 is recording.

[0097]the data (what is called.) for which the utilization condition conversion program 176 shows the utilization condition of the contents which the application program 54-1 for purchase received from EMD server 4-1 via the network 2 Usage Rule, the data which the application program 54-2 for purchase shows the utilization condition of the contents which received from EMD server 4-2, The application program 54-3 for purchase or the data in which the utilization condition of the contents which received from EMD server 4-3 is shown, It changes into the same format as the utilization condition data stored in the utilization condition file 202-1 thru/or 202-N which the contents database 53 is recording.

[0098]When the utilization condition conversion program 176 checks out contents to the portable device 12-1 or 12-3, The data of the utilization condition corresponding to the contents to check out is changed into the portable device 12-1 or the data of a

utilization condition with available 12-3.

[0099]Before the signature control program 177 performs processing of check-in or check-out, The alteration of the data of a utilization condition is detected based on the signature included in the data of the utilization condition stored in the utilization condition file 202-1 thru/or 202-N currently recorded on the contents database 53. The signature control program 177 updates the signature included in the data of a utilization condition corresponding to updating in the data of the utilization condition stored in the utilization condition file 202-1 thru/or 202-N accompanying processing of check-in or check-out currently recorded on the contents database 53.

[0100]The authentication program 178 Processing of the mutual recognition of the contents managing program 51 and the application program 54-1 for purchase, Processing of the mutual recognition of the contents managing program 51 and the application program 54-2 for purchase and processing of the mutual recognition of the contents managing program 51 and the application program 54-3 for purchase are performed. The authentication program 178 Processing of the mutual recognition of EMD server 4-1 and the application program 54-1 for purchase, The authentication key used by processing of the mutual recognition of EMD server 4-2 and the application program 54-2 for purchase and processing of the mutual recognition of EMD server 4-3 and the application program 54-3 for purchase is memorized.

[0101]The authentication key which the authentication program 178 uses by processing of mutual recognition, When the contents managing program 51 is installed in the personal computer 1, When the authentication program 178 does not memorize but processing of registration is normally performed by the display operation instruction program 52, it is supplied from the registration server which is not illustrated and the authentication program 178 memorizes.

[0102]The decoding program 179 decodes contents, when the personal computer 1-1 reproduces the contents stored in the contents file 201-1 thru/or 201-N which the contents database 53 is recording.

[0103]When the driver 180 for PD checks out predetermined contents to the portable device 12-2, Or when you check in at predetermined contents from the portable device 12-2, the command which makes the portable device 12-2 perform predetermined processing to contents or the portable device 12-2 is supplied.

[0104]When the driver 180 for PD checks out predetermined contents to the portable device 12-1, Or when you check in at predetermined contents from the portable device 12-1, the command which makes contents or the device driver 152-1 perform predetermined processing is supplied to the device driver 152-1.

[0105]When the driver 180 for PD checks out predetermined contents to the portable device 12-3, Or when you check in at predetermined contents from the portable device 12-3, the command which makes contents or the device driver 152-2 perform predetermined processing is supplied to the device driver 152-2.

[0106]The display operation instruction program 52 The filtering data file 221, the display data file 222, the graphics file 223-1, or 223-K, Or the picture of a predetermined window is displayed on the display 80 based on the history data file 224, and execution of processings, such as check-in or check-out, is directed based on the operation to the keyboard 78 or the mouse 79 at the contents managing program 51.

[0107]The filtering data file 221 stores the data for making weighting each contents stored in the contents file 201-1 thru/or 201-N currently recorded on the contents database 53, and is recorded on HDD81.

[0108]The display data file 222 stores the data corresponding to the contents stored in the contents file 201-1 thru/or 201-N currently recorded on the contents database 53, and is recorded on HDD81.

[0109]The graphics file 223-1 thru/or 223-K store the contents file 201-1 currently recorded on the contents database 53 thru/or the picture corresponding to 201-N, or the picture corresponding to a package, and is recorded on HDD81.

[0110]The number of times by which the history data file 224 was checked out in the contents stored in the contents file 201-1 thru/or 201-N currently recorded on the contents database 53, Historical data, such as the number of times at which he checked in, and its date, are stored, and it is recorded on HDD81.

[0111]While the display operation instruction program 52 transmits ID of the contents managing program 51 memorized beforehand to the registration server which is not illustrated via the network 2 at the time of processing of registration, The key for attestation and the EMD selection program 171 are received from a registration server, and the key for attestation and the EMD selection program 171 are supplied to the contents managing program 51.

[0112]When directions of sound recording are inputted, the sound recording program 151 reads contents from CD which is the optical disc 92 with which the drive 82 was equipped, and outputs them to the contents managing program 51 with the data of the utilization condition corresponding to contents, such as the number of times of check-out maximum possible, etc.

[0113]The contents which the contents database 53 is compressed by the prescribed method supplied from the contents managing program 51, and are enciphered by the prescribed method are stored in either the contents file 201-1 thru/or 201-N (it records on HDD81). The contents database 53 the data of the utilization condition corresponding to the contents stored in the contents file 201-1 thru/or 201-N, respectively, It stores in either the contents file 201-1 in which contents are stored the utilization condition file 202-1 respectively corresponding to 201-N thru/or 202-N (it records on HDD81).

[0114]The contents database 53 may record the contents file 201-1 thru/or 201-N or the utilization condition file 202-1 thru/or 202-N as a record.

[0115]For example, the data of the utilization condition corresponding to the contents stored in the contents file 201-1 is stored in the utilization condition file 202-1. The data of the utilization condition corresponding to the contents stored in contents file 201-N is stored in utilization condition file 202-N.

[0116]When, as for the boot program 117, the operating system of the personal computer 1-1 is operating, When the signal of the purport that are what is called a resident program and the portable device 12-1 was connected to USB port 83-1 from the device driver 152-1 which is always operating is received, When the display operation instruction program 52 is not started, the display operation instruction program 52 is started.

[0117]The boot program 117 starts the display operation instruction program 52, when the signal of the purport that the portable device 12-3 was connected to USB port 83-3 from the device driver 152-2 is received and the display operation instruction program 52 is not started.

[0118]Hereafter, when it is not necessary to distinguish the contents file 201-1 thru/or 201-N separately, the contents file 201 is only called. Hereafter, when it is not necessary to distinguish the utilization condition file 202-1 thru/or 202-N separately, the utilization condition file 202 is only called.

[0119]Since the composition of the function of the personal computer 1-2 is the same as the composition of the function of the personal computer 1-1, the explanation is omitted.

[0120]Hereafter, when it is not necessary to distinguish the personal computer 1-1 and 1-2 separately, the personal computer 1 is only called.

[0121]Drawing 6 is a figure explaining the contents which the personal computer 1 is recording. The application program 54-1 for purchase receives the contents enciphered with the contents key from EMD server 4-1 with a contents key, and supplies the contents which received to the contents managing program 51 via SAC. The application program 54-1 for purchase decodes the contents key enciphered with the session key etc., and supplies it to the contents managing program 51.

[0122]The application program 54-2 for purchase receives the contents enciphered with the contents key from EMD server 4-2 with a contents key, and supplies the contents which received to the contents managing program 51 via SAC. The application program 54-2 for purchase decodes the contents key enciphered with the session key etc., and supplies it to the contents managing program 51.

[0123]The application program 54-3 for purchase receives the contents enciphered with the contents key from EMD server 4-3 with a contents key, and supplies the contents which received to the contents managing program 51 via SAC. The application program 54-3 for purchase decodes the contents key enciphered with the session key etc., and supplies it to the contents managing program 51.

[0124]The group gateway programs 61 At the time of processing of the registration to

the recognition server 3. While transmitting ID of the contents managing program 51 and the number of a credit card which have been beforehand memorized to the recognition server 3 via the network 2, a group key, ID, and a password are received from the recognition server 3.

[0125]The contents managing program 51 has memorized the storage key 253 to secure one beforehand. The contents key supplied from the application program 54-1 for purchase with the storage key 253 according to the demand from the display operation instruction program 52. The contents key supplied from the application program 54-2 for purchase or the contents key supplied from the application program 54-3 for purchase is enciphered.

[0126]The contents managing program 51 is made to record on the contents database 53 by making into the contents file 201 the contents key 252 enciphered with the contents 251 and the storage key 253 which are enciphered with the contents key.

[0127]Drawing 7 is a figure explaining the contents which the personal computer 1 outputs. The group gateway programs 61 of the application program 54-3 for purchase require the contents 251-1 of the contents managing program 51.

[0128]The contents managing program 51 reads the contents 251-1 and the contents key 252 from the contents database 53. The contents managing program 51 is supplied to the group gateway programs 61 with the contents 251-1 which decode the contents key 252 with the memorized storage key 253, and are enciphered with the contents key.

[0129]The group gateway programs 61 output the contents 251-2 enciphered with the contents key with the contents key 272 which enciphers the decoded contents key with the group key 271, and is enciphered with the group key 271.

[0130]Since it is enciphered with the contents key and the contents key 272 is enciphered with the group key 271, if the contents 251-2 outputted from the personal computer 1 remain as it is, the contents 251-2 cannot be used for them.

[0131]Operation of the personal computer 1-2 which imports the contents 251-2 outputted from the personal computer 1-1 is explained with reference to drawing 8.

[0132]The group gateway programs 61-2 of the personal computer 1-2 decode the contents key 272 with the group key 271-2 memorized beforehand, when right ID and a password are entered and recognition is acquired from the recognition server 3.

[0133]The group key 271-2 which the group gateway programs 61-2 have memorized is the same as the group key 271-1 which the group gateway programs 61-1 have memorized.

[0134]The group gateway programs 61-2 supply the contents 251-2 enciphered with the decoded contents key and the contents key to the contents managing program 51-2.

[0135]With the contents key 252-2 which the contents managing program 51-2 enciphers a contents key with the storage key 253-2, and is enciphered with the

storage key 253-2. The contents 251-3 enciphered with the contents key are made to record on the contents database 53-2.

[0136]When using the contents 251-3 which the personal computer 1-2 was outputted from the personal computer 1-1, and were imported, The contents of a plaintext can be obtained by decoding the contents key 252-2 with the storage key 51-2, and decoding the contents 251-3 with the decoded contents key.

[0137]Thus, it is claimed that the personal computer 1-1 and the personal computer 1-2 which have the group key 271-1 which has the same value, or 271-2 belong to the same group.

[0138]The group key 271-1 which has the same value, or 271-2 is supplied from the recognition server 3 at the time of registration.

[0139]As shown in drawing 9, the personal computer 1-2 belonging to the same group as the personal computer 1-1 can import the contents outputted from the personal computer 1-1, when recognized from the recognition server 3.

[0140]However, the personal computer 281 which does not belong to the same group as the personal computer 1-1 cannot import the contents outputted from the personal computer 1-1, and cannot use them.

[0141]Drawing 10 is a figure explaining the processing which registers the personal computer 1-1 belonging to one group thru/or 1-3 into the recognition server 3.

[0142]When registering the 1st personal computer 1-1 belonging to one group into the recognition server 3, the personal computer 1-1, With ID of the contents managing program 51 of the personal computer 1-1, the number of a credit card, a user's name, a user's mail address, etc. are transmitted to the recognition server 3. The recognition server 3 registers the personal computer 1-1 and a user by recording [ mail address / ID of the contents managing program 51 which received from the personal computer 1-1, the number of a credit card, a user's name, / of a user ]. When registration is completed, the recognition server 3 transmits the group key 271 to the personal computer 1-1 with a group's ID and password. The personal computer 1-1 memorizes the group key 271 received from the recognition server 3.

[0143]ID of the group whom the recognition server 3 transmits is a number of a user's credit card. Or the password which the recognition server 3 transmits is a number of a user's credit card.

[0144]Since a possibility that a user will suffer an unexpected disadvantage will become high by doing in this way if other persons get to know a group's ID or password, the user who uses the personal computer 1 belonging to a group does not inform other persons of a group's ID and password. Therefore, it becomes possible to use by two or more apparatus, without using unjustly the contents outputted from the personal computer 1-1.

[0145]When registering into the recognition server 3 the 2nd personal computer 1-2 belonging to the group to whom the personal computer 1-1 belongs, the personal

computer 1-2 transmits ID of the contents managing program 51 of the personal computer 1-2, etc. to the recognition server 3. The recognition server 3 registers the personal computer 1-2 by recording [ ID / which received from the personal computer 1-2 / of the contents managing program 51 ]. The recognition server 3 transmits the group key 271 to the personal computer 1-2. The personal computer 1-2 memorizes the group key 271 received from the recognition server 3.

[0146]When registering into the recognition server 3 the 3rd personal computer 1-3 belonging to the group to whom the personal computer 1-1 belongs, the personal computer 1-3 transmits ID of the contents managing program 51 of the personal computer 1-3, etc. to the recognition server 3. The recognition server 3 registers the personal computer 1-3 by recording [ ID / which received from the personal computer 1-3 / of the contents managing program 51 ]. The recognition server 3 transmits the group key 271 to the personal computer 1-3. The personal computer 1-3 memorizes the group key 271 received from the recognition server 3.

[0147]Thus, the personal computer 1-1 belonging to the same group thru/or 1-3 memorize the same group key 271.

[0148]Drawing 11 is a figure explaining processing when importing contents. The personal computer 1-2 requires a group's ID and the input of a password, when importing the contents supplied from the personal computer 1-1, and it requires recognition of the recognition server 3.

[0149]The personal computer 1-2 performs import of the contents supplied from the personal computer 1-1, when a right group's ID and password are entered and it is recognized by the recognition server 3.

[0150]Next, with reference to the flow chart of drawing 12, processing of registration by the personal computer 1 and the recognition server 3 which execute the group gateway programs 61 is explained.

[0151]In Step S1101, the group gateway programs 61 acquire the number of the credit card inputted by operation of the keyboard 78 etc. In Step S1102, the group gateway programs 61 acquire ID from the contents managing program 51, and transmit ID of the contents managing program 51, and the number of a credit card to the recognition server 3 via the network 2.

[0152]In Step S2101, the recognition server 3 receives ID of the contents managing program 51 and the number of a credit card which were transmitted from the personal computer 1. In Step S2102, the recognition server 3, Based on the number of a credit card, etc., it is judged whether the personal computer 1 is a group's 1st personal computer, When judged with the personal computer 1 being a group's 1st personal computer, it progresses to Step S2103 and the group key 271 is generated. In Step S2104, the recognition server 3 generates ID or the password of the same group as the number of a credit card, for example.

[0153]In Step S2105, the recognition server 3 generates the account corresponding

to a user, and procedure follows it to Step S2106.

[0154] In Step S2102, the personal computer 1 is not a group's 1st personal computer. That is, since processing of generation of the group key 271 and account is unnecessary when judged with it being the personal computer 1 after the 2nd set, processing of Step S2103 thru/or Step S2105 is skipped, and procedure progresses to Step S2106.

[0155] In Step S2106, the recognition server 3 registers ID of the contents managing program 51. In Step S2107, the recognition server 3 transmits the group key 271, a group's ID, and a password to the personal computer 1 via the network 2.

[0156] In Step S1103, the group gateway programs 61 receive the group key 271 transmitted from the recognition server 3, a group's ID, and a password. In Step S1104, the group gateway programs 61 record the group key 271, a group's ID, and a password. In Step S1105, the group gateway programs 61 display a group's ID and a password on the display 80, and end processing.

[0157] Thus, the personal computer 1-1 can acquire the group key 271, a group's ID, and a password by transmitting ID of the contents managing program 51, and the number of a credit card to the recognition server 3. On the other hand, with a group's ID which the recognition server 3 acquired ID of the contents managing program 51, and the number of the credit card on the occasion of registration of the personal computer 1, and was generated, and a password. ID of the contents managing program 51 and the number of a credit card which were acquired are recordable.

[0158] Next, ID of the group corresponding to processing of Step S2104 of drawing 12 and the example of processing of generation of a password are explained with reference to the flow chart of drawing 13.

[0159] In Step S11, the recognition server 3 acquires the number of the received credit card. In Step S12, the recognition server 3 generates a group's ID and password. In processing of Step S12, a group's ID and either of the passwords which are generated are the same as that of the number of a credit card.

[0160] In Step S13, the recognition server 3 makes the number of a credit card, a group's ID, and a password correspond, is recorded, and ends processing.

[0161] Thus, since a group's ID and either of the passwords which are generated by the recognition server 3 are the same as that of the number of a credit card, a group's ID and password are prevented from being widely known by others.

[0162] Next, processing of the output of the contents of the personal computer 1 is explained with reference to the flow chart of drawing 14.

[0163] In Step S31, the contents managing program 51 reads the contents 251 and the contents key 252 from the contents database 53. The contents 251 are enciphered with the contents key and the contents key 252 is enciphered with the storage key 253.

[0164] In Step S32, the contents managing program 51 decodes the contents key 252



with the memorized storage key 253. The contents managing program 51 supplies the contents 251 enciphered with the contents key, and the contents key of a plaintext to the group gateway programs 61.

[0165]In Step S33, the group gateway programs 61 are the group keys 271 memorized beforehand, encipher a contents key and generate the contents key 272.

[0166]In Step S34, the group gateway programs 61 output the contents 251 enciphered with the contents key, and the contents key 272 enciphered with the group key 271, and end processing.

[0167]Thus, the personal computer 1 can output the contents 251 enciphered with the contents key, and the contents key 272 enciphered with the group key 271.

[0168]Next, the processing which imports the contents 251 of the personal computer 1 is explained with reference to the flow chart of drawing 15. In Step S1201, the group gateway programs 61, The contents 251 enciphered with the contents key and the contents key 272 enciphered with the group key 271 are acquired via recording media, such as the magneto-optical disc 93, via the network 2. In Step S1202, the group gateway programs 61 acquire a group's ID and password corresponding to operation of the keyboard 78 etc.

[0169]In Step S1203, the group gateway programs 61, Based on ID and the password of the group who has memorized, it is judged whether a group's ID and password which were acquired by processing of Step S1202 are the right, When a group's ID and password are judged to be the right, it progresses to Step S1204 and a group's ID and password are transmitted to the recognition server 3 via the network 2.

[0170]In Step S2201, the recognition server 3 receives a group's ID and password which were transmitted from the personal computer 1. In Step S2202, the recognition server 3, Based on a group's ID and password which are recorded, it is judged whether ID and the password of the group who received by processing of Step S2201 are the right, When a group's ID and password are judged to be the right, it progresses to Step S2203 and the data of the purport that the personal computer 1 is recognized is transmitted via the network 2.

[0171]In Step S1205, the group gateway programs 61 receive the data of the purport that it recognizes transmitted from the recognition server 3. In Step S1206, the group gateway programs 61 decode the contents key 272 with the group key 271. The group gateway programs 61 supply the decoded contents key to the contents managing program 51. In Step S1207, the contents managing program 51 enciphers a contents key with the storage key 253. In Step S1208, the contents managing program 51 records the contents 251 enciphered with the contents key, and the contents key 252 enciphered with the storage key 253 on the contents database 53, and ends processing of import.

[0172]In Step S1203, since import of the contents 251 cannot be permitted when judged with a group's ID and password not being right, processing is ended, without

recording the contents 251 on the contents database 53.

[0173]In Step S2202, since the personal computer 1 cannot be recognized when judged with a group's ID and password not being right, processing is ended, without recording the contents 251 on the contents database 53.

[0174]Thus, the personal computer 1 imports the contents 251, when right ID and a bus word are inputted and it is recognized by the recognition server 3.

[0175]Drawing 16 is a figure explaining other examples of a group's ID and the controlling method of a password.

[0176]In processing of registration, the personal computer 1 transmits accounting information, such as a number of a credit card, to the recognition server 3. The recognition server 3 transmits the number of a credit card to the ID management server 8, and acquires a group's ID and password from the ID management server 8.

[0177]When the ID management server 8 receives the number of the credit card for the first time from the recognition server 3, A group's ID and password including the number of a credit card are generated, make it correspond to the number of a credit card, and a group's ID and password are recorded, and a group's ID and password are transmitted to the recognition server 3. When the number of the credit card which the ID management server 8 received from the recognition server 3 is already recorded. (When [ for example, ] already registered by EMD server 4), ID and the password which are registered corresponding to the number of a credit card are transmitted to the recognition server 3 as a group's ID and password.

[0178]The recognition server 3 transmits a group's ID and password to the personal computer 1.

[0179]When the ID management server 8 receives the number of the credit card for the first time from EMD server 4, ID and a password including the number of a credit card are generated, make it correspond to the number of a credit card, and ID and a password are recorded, and ID and a password are transmitted to EMD server 4. The ID management server 8 transmits ID and the password which are registered corresponding to the number of a credit card to EMD server 4, when the number of the credit card received from EMD server 4 is recorded (for example, when already registered by the recognition server 3).

[0180]EMD server 4 transmits ID and a password to the personal computer 1.

[0181]After registering [ doing in this way ] with the recognition server 3, even if it registers with EMD server 4, after registering with EMD server 4, even if it registers with the recognition server 3, it becomes the same as that of ID and the password with which the group's ID and password registered with EMD server 4 in any case.

[0182]Therefore, a group's ID and the user who knows the password only enter a group's ID and password, and can purchase contents from EMD server 4. Based on a group's ID and password which were entered, EMD server 4 which sold contents reads the number of a credit card from the ID management server 8, and performs

processing of the fee collection to the purchase of contents.

[0183]Since a possibility that a user will suffer an unexpected disadvantage will become high by doing in this way if other persons get to know a group's ID and password, the user who uses the personal computer 1 belonging to a group does not inform other persons of a group's ID and password. Therefore, it becomes possible to use by two or more apparatus, without using unjustly the contents outputted from the personal computer 1.

[0184]Next, processing of registration in case the ID management server 8 generates ID and a password is explained with reference to the flow chart of drawing 17.

[0185]In Step S1301, the group gateway programs 61 acquire the number of the credit card inputted by operation of the keyboard 78 etc. In Step S1302, the group gateway programs 61 acquire ID from the contents managing program 51, and transmit ID of the contents managing program 51, and the number of a credit card to the recognition server 3 via the network 2.

[0186]In Step S2301, the recognition server 3 receives ID of the contents managing program 51 and the number of a credit card which were transmitted from the personal computer 1. In Step S2302, the recognition server 3, Based on the number of a credit card, etc., it is judged whether the personal computer 1 is a group's 1st personal computer, When judged with the personal computer 1 being a group's 1st personal computer, it progresses to Step S2303 and the group key 271 is generated. In Step S2304, the recognition server 3 transmits the number of a credit card to the ID management server 8 via the network 2.

[0187]In Step S3301, the ID management server 8 receives the number of a credit card. In Step S3302, the ID management server 8 performs processing of generation of ID and a password. In Step S3303, the ID management server 8 transmits ID and a password to the recognition server 3 via the network 2.

[0188]In Step S2305, the recognition server 3 receives ID and a password. In Step S2306, the recognition server 3 generates the account corresponding to a user, and procedure follows it to Step S2307.

[0189]. In Step S2302, the personal computer 1 is not a group's 1st personal computer. That is, since processing of generation of the group key 271 and account is unnecessary when judged with it being the personal computer 1 after the 2nd set, processing of Step S2303 thru/or Step S2306 is skipped, and procedure progresses to Step S2307.

[0190]Since each of processing of Step S2307 thru/or Step S1305 is the same as that of each of the processing of Step S2106 thru/or Step S1105 shown in drawing 12, the explanation is omitted.

[0191]Next, the example of processing of generation of ID by the ID management server 8 corresponding to processing of Step S3302 of drawing 17 and a password is explained with reference to the flow chart of drawing 18.

[0192]In Step S51, it progresses to Step S52 and the ID management server 8 generates ID and a password, when it judges whether the number of the credit card acquired by processing of reception is registered and is judged with the number of a credit card not being registered. In processing of Step S52, a group's ID and either of the passwords which are generated are the same as that of the number of a credit card.

[0193]In Step S53, the ID management server 8 makes a number, and ID and the password of a credit card correspond, is recorded, and ends processing.

[0194]In Step S51, when judged with the number of a credit card being registered, it progresses to Step S54, and the ID management server 8 reads ID and the password which are recorded corresponding to the number of a credit card, and ends processing.

[0195]Next, processing of registration by the personal computer 1 and EMD server 4 is explained with reference to the flow chart of drawing 19. In Step S1401, the personal computer 1 acquires the number of a credit card corresponding to operation of the keyboard 78 etc. In Step S1402, the personal computer 1 transmits the number of a credit card to EMD server 4 via the network 2.

[0196]In Step S2401, EMD server 4 receives the number of the credit card which the personal computer 1 transmitted. In Step S2402, EMD server 4 transmits the number of a credit card to the ID management server 8 via the network 2.

[0197]In Step S3401, the ID management server 8 receives the number of the credit card which EMD server 4 transmitted. In Step S3402, the ID management server 8 generates ID and a password. Since the details of processing of Step S3402 are the same as that of the processing explained with reference to the flow chart of drawing 18, the explanation is omitted.

[0198]In Step S3403, the ID management server 8 transmits ID and a password to EMD server 4 via the network 2.

[0199]In Step S2403, EMD server 4 receives ID and a password. In Step S2404, EMD server 4 generates account. In Step S2405, EMD server 4 transmits ID and a password to the personal computer 1 via the network 2.

[0200]In Step S1403, the personal computer 1 receives ID and a password. In Step S1404, the personal computer 1 displays ID and the password which were received, and ends processing.

[0201]Thus, a group's ID and password which the recognition server 3 publishes can be made common with ID and the password which EMD server 4 publishes.

[0202]Next, processing of the settlement of accounts performed when contents are purchased from EMD server 4 is explained with reference to the flow chart of drawing 20. In Step S1501, the personal computer 1 acquires ID and the password which were registered into the group's ID and password, or EMD server 4, and were acquired corresponding to operation of the keyboard 78 etc. In Step S1502, the personal computer 1 transmits the demand of settlement of accounts to EMD server 4 with ID

and a password via the network 2.

[0203]In Step S2501, EMD server 4 receives ID transmitted from the personal computer 1, a password, and the demand of settlement of accounts. In Step S2502, EMD server 4 transmits ID and a password to the ID management server 8 via the network 2.

[0204]In Step S3501, the ID management server 8 receives ID and the password which were transmitted from EMD server 4. In Step S3502, the ID management server 8 reads the credit card number corresponding to ID and a password. In Step S3503, the ID management server 8 transmits a credit card number to EMD server 4 via the network 2.

[0205]In Step S2503, EMD server 4 receives a transmitting \*\*\*\* credit card number from the ID management server 8. In Step S2504, based on the received credit card number, EMD server 4 performs processing of fee collection, and ends processing.

[0206]Thus, EMD servers 4 are either [ which was registered into a group's ID and the password, or EMD server 4, and was acquired ] ID and a password, and can perform processing of fee collection.

[0207]Next, the personal computer 1 explains other processings which import contents with reference to drawing 21.

[0208]In this example, when it registers with the recognition server 3, the group gateway programs 61 of the personal computer 1 do not acquire a group key, but acquire only a group's ID and password.

[0209]The group gateway programs 61 transmit a group's ID and password to the decipherment authentication server 331 via the network 2, when import of the contents 251 is required and a group's ID and password are entered by the user. The decipherment authentication server 331 will transmit a group's ID and password to the recognition server 3 further, if a group's ID and password which were transmitted from the personal computer 1 are received.

[0210]If a group's ID and password which were transmitted from the decipherment authentication server 331 are received, the recognition server 3, Based on a group's ID and password which have been recorded beforehand, it judges whether ID and the password of the group who received are the right, and the decision result is transmitted to it at the decipherment authentication server 331.

[0211]When a group's ID and password are judged to be the right, based on a group's ID and password, the decipherment authentication server 331 generates the group key 271, and transmits the group key 271 to the personal computer 1 via the network 2.

[0212]On the other hand, when judged with a group's ID and password not being right, the decipherment authentication server 331 ends processing without generating the group key 271.

[0213]Thus, when generation of the group key 271 is required based on a group's ID

and password which became invalid for a certain reason, for example, the decipherment authentication server 331 does not generate the group key 271.

[0214]Since the decipherment authentication server 331 generates the group key 271 whenever contents are decoded, it can know the using state of contents.

[0215]As mentioned above, since it does not have the procedure which the group gateway programs 61 do not hold the group key 271, and generates the group key 271, the personal computer 1 can prevent unjust import of the contents 251 more firmly.

[0216]With reference to the flow chart of drawing 22, processing of transmission of the group key 271 which the decipherment authentication server 331 performs is explained. In Step S71, the decipherment authentication server 331 receives a group's ID and password which were transmitted from the personal computer 1 via the network 2. In Step S72, the decipherment authentication server 331, A group's ID and password are transmitted to the recognition server 3, it asks the recognition server 3 whether a group's ID and password are just, and the data in which it is shown from the recognition server 3 whether a group's ID and password are just is received.

[0217]In Step S73, the decipherment authentication server 331, When it judges whether a group's ID and password are just and is judged with a group's ID and password being just based on the data received from the recognition server 3, it progresses to Step S74 and the group key 271 is generated based on a group's ID and password. In Step S75, the decipherment authentication server 331 transmits the generated group key 271 to the personal computer 1 via the network 2, and ends processing.

[0218]In Step S73, since import cannot be permitted when judged with a group's ID and password not being just, the decipherment authentication server 331 ends processing without transmitting the group key 271 to the personal computer 1.

[0219]Thus, when the decipherment authentication server 331 receives a group's ID and password from the personal computer 1 and a group's ID and password are just, The group key 271 is generated, it transmits to the personal computer 1, and when a group's ID and password are not just, the group key 271 is not generated. Therefore, the personal computer 1 can be restricted to the time when the just group's ID and password were entered, and can import the contents 251.

[0220]Next, operation of the locker server 11 is explained.

[0221]Drawing 23 is a figure explaining processing of the registration to the locker server 11. It is connected with the contents database 401 and the locker server 11 is connected with the log database 402.

[0222]The locker server 11 is made to record on the contents database 401 supplied from the personal computer 1 via the network 2.

[0223]The contents database 401 records the contents which the locker server 11 received from the personal computer 1 registered, and supplies the contents currently recorded to the locker server 11 corresponding to the demand from the locker server

11.

[0224]The locker server 11 transmits the contents supplied from the contents database 401 to the personal computer 1 via the network 2.

[0225]The log database 402 records the log corresponding to processing of registration of the personal computer 1 to the locker server 11, processing of record of contents, or processing of read-out of contents.

[0226]The personal computer 1 transmits the number of a credit card to the locker server 11, when requiring the registration to the locker server 11.

[0227]The locker server 11 generates ID, and makes generated ID record on the log database 402, and it transmits generated ID to the personal computer 1. ID which the locker server 11 generates is the same as that of the number of the credit card of the user of the personal computer 1, for example.

[0228]The locker server 11 transmits the log which shows that the personal computer 1 was registered to the personal computer 1, and performs processing of the fee collection corresponding to registration, and transmits the result to the personal computer 1.

[0229]Drawing 24 is a figure explaining the example of the list of contents which the locker server 11 is recording. The locker server 11 is made to correspond to ID of the user who has registered, and records the name of contents.

[0230]For example, the locker server 11 is made to correspond to ID of the user who is "aaaaa", The name of the contents which are "IIIII" is recorded, it is made to correspond to ID of the user who is "bbbbb", and the name of the contents which are "RORORORORO" is recorded, it is made to correspond to ID of the user who is "ccccc", and the name of the contents which are "HAHAHAHAHA" is recorded.

[0231]Drawing 25 is a figure explaining common use of the contents by the locker server 11. The locker server 11 makes the contents supplied from the personal computer 1-1 record on the contents database 401. Make the list of contents correspond to ID of the user of the personal computer 1-1, and the locker server 11 records the name of contents on it, and. The log of a purport which made the contents supplied from the personal computer 1-1 record on the contents database 401 is made to record on the log database 402.

[0232]When transmission of contents is required from the personal computer 1-2 based on the same ID as the personal computer 1-1, the locker server 11, When it judges whether a user's ID is the right and a user's ID is judged based on the list of contents to be the right, supply of contents is required of the contents database 401. The locker server 11 transmits the contents supplied from the contents database 401 to the personal computer 1-2. The locker server 11 makes the log which shows having supplied contents to the personal computer 1-2 record on the log database 402.

[0233]The personal computer 1-1 can transmit the contents purchased from EMD server 4 to the locker server 11, and can also be made to record them on the

contents database 401, as shown in drawing 26. When transmission of contents is required from the personal computer 1-2 based on the same ID as the personal computer 1-1 also in this case, the locker server 11, Based on the same ID as the personal computer 1-1, supply of contents is required of the contents database 401, and the contents supplied from the contents database 401 are transmitted to the personal computer 1-2.

[0234]The locker server 11 transmits the log which shows that the personal computer 1 was registered to the personal computer 1, and it performs processing of monthly fee collection corresponding to registration, and it may be made to transmit the result to the personal computer 1, as shown in drawing 27.

[0235]Next, with reference to the flow chart of drawing 28, processing of registration by the personal computer 1 and the locker server 11 is explained.

[0236]In Step S1601, the personal computer 1 acquires the number of the credit card inputted by operation of the keyboard 78 etc. In Step S1602, the personal computer 1 transmits the number of a credit card to the locker server 11 via the network 2.

[0237]In Step S2601, the locker server 11 receives the number of the credit card transmitted from the personal computer 1. In Step S2602, the locker server 11 judges whether it was registered for the first time based on the number of the received credit card, and when judged with having been registered for the first time, it progresses to Step S2603 and it generates a user's ID. In Step S2604, the locker server 11 records a user's generated ID, and follows it to Step S2605.

[0238]In Step S2602, since processing of generation of ID is unnecessary when judged with not having been registered for the first time, processing of Step S2603 and processing of Step S2604 are skipped, and procedure progresses to Step S2605.

[0239]The locker server 11 makes the log of a purport which registered the user's ID record on the log database 402 in Step S2605. In Step S2606, the locker server 11 transmits a user's ID and a log to the personal computer 1 via the network 2.

[0240]In Step S1603, the personal computer 1 receives ID of the user transmitted from the locker server 11, and a log. In Step S1604, the personal computer 1 records a user's ID and a log. In Step S2607, the locker server 11, It judges whether based on the number of the received credit card, it was registered for the first time, and when judged with having been registered for the first time, based on the number of the credit card which he followed to Step S2608 and was received, processing of fee collection is performed and processing is ended.

[0241]In Step S2607, since processing of fee collection is unnecessary when judged with not having been registered for the first time, processing of Step S2608 is skipped and processing is ended.

[0242]Thus, the personal computer 1 can acquire a user's ID by transmitting the number of a credit card to the locker server 11. On the other hand, the locker server 11 can record the number of the credit card acquired with ID of the user who acquired



and generated the number of the credit card in the case of registration of the personal computer 1.

[0243]Next, with reference to the flow chart of drawing 29, processing of record of the contents to the locker server 11 is explained. In Step S1701, the personal computer 1 transmits contents to the locker server 11 with a user's ID via the network 2.

[0244]In Step S2701, the locker server 11 receives a user's ID and contents which were transmitted from the personal computer 1. In Step S2702, the locker server 11, When judged with judging whether ID of the user who received is registered based on a user's ID currently recorded on the list, and ID of the user who received being registered, the contents which progressed to Step S2703 and received are made to record on the contents database 401.

[0245]The locker server 11 makes the log of the purport that contents were recorded record on the log database 402 in Step S2704. In Step S2705, the locker server 11 transmits the log of the purport that contents were recorded to the personal computer 1 via the network 2.

[0246]In Step S1702, the personal computer 1 receives the log of the purport that contents were recorded transmitted from the locker server 11. In Step S1703, the personal computer 1 records the log which received. In Step S1704, the personal computer 1 displays the log which received on the display 80, and ends processing.

[0247]In Step S2702, since it is a demand of record of inaccurate contents when judged with ID of the user who received not being registered, processing is ended without recording contents.

[0248]Thus, the locker server 11 makes contents record on the contents database 401, when contents are received with right ID, and when contents are received with inaccurate ID, it cancels the contents which received.

[0249]Next, with reference to the flow chart of drawing 30, processing of read-out of the contents from the locker server 11 is explained. In Step S1801, the personal computer 1 transmits the demand of contents to the locker server 11 with a user's ID via the network 2.

[0250]In Step S2801, the locker server 11 receives a user's ID and the demand of contents which were transmitted from the personal computer 1. In Step S2802, the locker server 11, When judged with judging whether ID of the user who received is registered based on a user's ID currently recorded, and ID of the user who received being registered, it progresses to Step S2803 and contents are read from the contents database 401.

[0251]The locker server 11 makes the log corresponding to read-out of contents record on the log database 402 in Step S2804. In Step S2805, the locker server 11 transmits the log of the purport that the read contents and contents began to read to the personal computer 1 via the network 2.

[0252]In Step S1802, the personal computer 1 receives the contents and the log

which were transmitted from the locker server 11. In Step S1803, the personal computer 1 records the contents and the log which received. In Step S1804, the personal computer 1 displays the log which received on the display 80, and ends processing.

[0253]In Step S2802, since it is the demand of inaccurate contents when judged with ID of the user who received not being registered, processing is ended without transmitting contents.

[0254]Thus, the locker server 11 does not carry out contents transmission, when contents are read from the contents database 401, the read contents are transmitted, when the demand of contents is received with a user's ID registered, and the user's ID is not registered.

[0255]Next, a 2nd embodiment of the music data managerial system concerning this invention is described.

[0256]Drawing 31 is a figure showing a 2nd embodiment of the music data managerial system concerning this invention. In the public network 503, via the base station 502-1 which is a fixed-wireless-access office arranged at the cell divided into the size of the request of the offer area of communications service, respectively thru/or 502-4, PDA501-1, 501-2, the digital cellular phone terminal 16-1 with a camera, or 16-2 is connected.

[0257]The base station 502-1 thru/or 502-4 PDA501-1 which is an ambulant radio station, 501-2, the digital cellular phone terminal 16-1 with a camera, and 16-2, For example, wireless connection is carried out by the code division multiple access called W-CDMA (Wideband-Code Division Multiple Access), The data communications of the large capacity data can be carried out at high speed in the data transfer rate of a maximum of 2 Mbps(es) using PDA501-1 which is an ambulant radio station, 501-2, the digital cellular phone terminal 16-1 with a camera and 16-2, and a 2-GHz frequency band.

[0258]PDA501-1, 501-2, the digital cellular phone terminal 16-1 with a camera, and 16-2, Since the data communications of the large capacity data can be carried out at high speed with the base station 502-1 thru/or 502-4 and a W-CDMA method, the data communications which attain to varieties, such as transmission and reception of contents, such as transmission and reception of not only a voice call but an E-mail, an inspection of a simple homepage, and a picture, can be performed.

[0259]PDA501-1, 501-2, the digital cellular phone terminal 16-1 with a camera, or 16-2, A browser program, the contents managing program 51, the group gateway programs 61, etc. are executed, and it is used for management of contents, or input and output of contents.

[0260]The base station 502-1 thru/or 502-4 are connected to the public network 503 via the wire circuit. The Internet, the network 2, the member line terminal equipment that is not illustrated, the computer network, the network in a company, etc. are

connected to the public network 503.

[0261]It is connected to the public network 503 and the Internet Service Provider's access server 504 is further connected to the contents server 505 which an Internet Service Provider holds.

[0262]The contents server 505 satisfies member line-terminal-equipment and PDA501-1, 501-2, the digital cellular phone terminal 16-1 with a camera, or the demand from 16-2, For example, contents, such as a simple homepage, are provided as a file of a compact HTML (HyperText Markup Language) method.

[0263]Many WWW (World Wide Web) servers 506-1 thru/or 506-N are connected to the network 2. According to the protocol of TCP (Transmission Control Protocol)/IP (Internet Protocol), WWW server 506-1 thru/or 506-N, It is accessed from member line-terminal-equipment and PDA501-1, 1-2, the digital cellular phone terminal 16-1 with a camera, and 16-2.

[0264]WWW server 506-1 thru/or 506-N perform the same processing as the recognition server 3, EMD server 4, the ID management server 8, or the locker server 11, and via the network 2, PDA501-1, 501-2, the digital cellular phone terminal 16-1 with a camera, or 16-2 is provided with contents etc., and contents are recorded, it transmits or ID etc. are managed.

[0265]Incidentally PDA501-1, 501-2, the digital cellular phone terminal 16-1 with a camera, and 16-2, Even the base station 502-1 thru/or 502-4 are communicated with the simple transport protocol of 2Mbps, and even the network 2 and WWW server 506-1 thru/or base station 502-1 thru/or 502-4 to 506-N are communicated by TCP/IP.

[0266]The supervisory control device 507 via the public network 503 Member line terminal equipment, It is connected to PDA501-1, 1-2, the digital cellular phone terminal 16-1 with a camera, and 16-2, Authenticating processing or accounting to member line-terminal-equipment and PDA501-1, 501-2, the digital cellular phone terminal 16-1 with a camera, and 16-2, etc. is performed.

[0267]The digital cellular phone terminal 16-1 with a camera and 16-2 use contents by the same processing as the personal computer 1 mentioned above via the public network 503 and the network 2.

[0268]Hereafter, when it is not necessary to distinguish the digital cellular phone terminal 16-1 with a camera, and 16-2 separately, the digital cellular phone terminal 16 with a camera is only called.

[0269]Next, the appearance composition of the digital cellular phone terminal 16 with a camera which applied this invention is explained. As shown in drawing 32, the digital cellular phone terminal 16 with a camera comprises the indicator 531 and the main part 532, and is formed of the central hinge region 533 so that folding is possible.

[0270]The indicator 531 has the antenna 534 for transmission and reception in which a cash drawer or storage is possible in an upper bed left part. The digital cellular

phone terminal 16 with a camera transmits and receives an electric wave via the antenna 534 between the base station 502-1 which is a fixed-wireless-access office thru/or either of 502-4.

[0271]The indicator 531 has the camera part 535 which can rotate freely in the upper bed center section in the angle range of about 180 degrees. The digital cellular phone terminal 16 with a camera picturizes the desired candidate for an image pick-up with CCD camera 536 of the camera part 535.

[0272]When the camera part 535 rotates about 180 degrees and is positioned by the user, as shown in drawing 33, the indicator 531 will be in the state where the loudspeaker 537 provided in the center of the back side of the camera part 535 is located in the transverse-plane side. Thereby, the digital cellular phone terminal 16 with a camera switches to the usual voice call state.

[0273]The liquid crystal display 538 is formed in the transverse plane of the indicator 531. The liquid crystal display 538 displays the picture etc. which were picturized with CCD camera 536 of the contents of the E-mail besides being a partner point name, a telephone number, a dispatch history which are registered as the receive state of an electric wave, battery residue, and a telephone directory, a simple homepage, and the camera part 535.

[0274]On the other hand, the operation keys 539, such as the numerical keypad of "0" thru/or "9", a call origination key, a redial key, clear back and a power key, a Clear key, and a mail key, are formed in the surface at the main part 532. The various directions corresponding to operation of the operation key 539 are inputted into the digital cellular phone terminal 16 with a camera.

[0275]MEMOBOTAN 540 and the microphone 541 are formed in the lower part of the operation key 539 of the main part 532. The digital cellular phone terminal 16 with a camera records the sound of the partner under telephone call, when MEMOBOTAN 540 is operated. The digital cellular phone terminal 16 with a camera collects the sound of the user at the time of a telephone call with the microphone 541.

[0276]The jog dial 542 which can rotate freely in the upper part of the operation key 539 of the main part 532 is formed in the state where it projected slightly from the surface of the main part 532. The digital cellular phone terminal 16 with a camera performs operation of versatility, such as a telephone directory list currently displayed on the liquid crystal display 538 or scroll operation of an E-mail, page \*\*\*\* operation of a simple homepage, or feeding operation of a picture, according to the rotating operation to the jog dial 542.

[0277]For example, the main part 532 chooses a desired telephone number out of two or more telephone numbers of the telephone directory list displayed on the liquid crystal display 538 according to the rotating operation of the jog dial 542 by a user. When the jog dial 542 is pressed by the internal direction of the main part 532, the telephone number chosen is become final and conclusive, and call origination

processing is automatically performed to the settled telephone number.

[0278]It is equipped with the battery pack which is not illustrated to the back side, and electric power will be supplied from a battery pack to each circuit part, and the main part 532 will start in the state where it can operate, if clear back/power key is turned on.

[0279]By the way, the memory card slot 543 for equipping with the memory card 13 which can be freely taken out and inserted in the upper part of the left lateral of the main part 532 is formed. The digital cellular phone terminal 16 with a camera will be recorded on the memory card 13 equipped with the sound of the partner under telephone call, if MEMOBOTAN 540 is pushed. The digital cellular phone terminal 16 with a camera is recorded on the memory card 13 equipped with contents, such as a picture picturized with the E-mail, the simple homepage, and CCD camera 536, or a sound, according to a user's operation.

[0280]The memory card 13 is a memory stick (trademark), for example. A memory stick is a kind of the flash memory card developed by Sony Corp. which is an applicant for this patent. This memory card 13, vertical 21.5 mm width 50 mm thickness 2.8 [mm]. In the plastic case of a \*\* small thin form. The flash memory element which is a kind of EEPROM (Electrically Erasable and Programmable Read OnlyMemory) which is the nonvolatile memory which can be rewritten and eliminated electrically is stored, Writing and read-out of a picture, a sound, music, etc. are possible via 10 pin terminals. [ various data ]

[0281]A memory stick also receives specification change of the built-in flash memory by large-scale-izing etc., The original serial protocol which can secure compatibility by the apparatus to be used is adopted, and it is the maximum writing speed 1.5 [MB/S]. High speed performance of the maximum read speed 2.45 [MB/S] is realized, and the erroneous deletion preventing switch was formed and high reliability is secured.

[0282]Therefore, since the digital cellular phone terminal 16 with a camera is constituted so that wearing of such a memory card 13 is possible, it can attain sharing of data among other electronic equipment via the memory card 13.

[0283]As shown in drawing 34, the digital cellular phone terminal 16 with a camera, As opposed to the main control part 551 which controls the indicator 531 and each part of the main part 532 in generalization, The power circuit part 552, the operational input control section 553, the image encoder 554, the camera interface part 555, the LCD (Liquid Crystal Display) control section 556, the image decoder 557, the demultiplexing part 558, the regeneration part 563, the strange demodulator circuit unit 559, And the voice codec 560 is mutually connected via the main bus 561, and via the synchronous bus 562, it is connected mutually and the image encoder 554, the image decoder 557, the demultiplexing part 558, the strange demodulator circuit unit 559, and the voice codec 560 are constituted.

[0284]The power circuit part 552 will start the digital cellular phone terminal 16 with a camera in the state where it can operate, by supplying electric power from a battery pack to each part, if clear back/power key is made an ON state by a user's operation.

[0285]In voice call mode, the digital cellular phone terminal 16 with a camera changes into digital sound data the audio signal which collected the sound with the microphone 541 by the voice codec 560 based on control of the main control part 551 which becomes by CPU, ROM, RAM, etc. The digital cellular phone terminal 16 with a camera carries out spectrum diffusion treatment of the digital sound data in the strange demodulator circuit unit 559, and after it performs digital-to-analog conversion processing and frequency conversion processing with the transmitting and receiving circuit section 564, it transmits via the antenna 534.

[0286]In voice call mode the digital cellular phone terminal 16 with a camera, The input signal received with the antenna 534 is amplified, frequency conversion processing and an analog-to-digital conversion process are performed, spectrum back-diffusion-of-gas processing is carried out in the strange demodulator circuit unit 559, and it changes into an analog voice signal by the voice codec 560. The digital cellular phone terminal 16 with a camera makes the sound corresponding to an analog voice signal output to the loudspeaker 537.

[0287]In data communication mode, the digital cellular phone terminal 16 with a camera sends out the contents specified by operation of the operation key 539 and the jog dial 542 corresponding to the input to the main control part 551, when transmitting contents.

[0288]The main control part 551 carries out spectrum diffusion treatment of the contents in the strange demodulator circuit unit 559, and after it performs digital-to-analog conversion processing and frequency conversion processing with the transmitting and receiving circuit section 564, it transmits to a base station via the antenna 534.

[0289]On the other hand, the digital cellular phone terminal 16 with a camera, In data communication mode, when receiving contents, spectrum back-diffusion-of-gas processing of the input signal received from base station CS3 via the antenna 534 is carried out in the strange demodulator circuit unit 559, After restoring the original contents, the data corresponding to contents is displayed on the liquid crystal display 538 via the LCD control section 556.

[0290]The LCD control section 556 is connected to the liquid crystal display 538 like the flexible printed wiring board 11 via the flexible printed wiring board which has a panel ID setting part.

[0291]Then, the digital cellular phone terminal 16 with a camera can also record the contents which received according to a user's operation on the memory card 13 via the regeneration part 563.

[0292]The digital cellular phone terminal 16 with a camera supplies the image data

picturized with CCD camera 536 to the image encoder 554 via the camera interface part 555, when transmitting image data in data communication mode.

[0293]Incidentally, the digital cellular phone terminal 16 with a camera can also display directly the image data picturized with CCD camera 536 on the liquid crystal display 538 via the camera interface part 555 and the LCD control section 556, when not transmitting image data.

[0294]The image encoder 554 the image data supplied from CCD camera 536, For example, by carrying out compression encoding with predetermined coding modes, such as MPEG(Movig Picture Experts Group) 2 or MPEG4, it changes into coded image data and this is sent out to the demultiplexing part 558.

[0295]At this time, the digital cellular phone terminal 16 with a camera sends out simultaneously the sound which collected the sound with the microphone 541 as digital voice data via the voice codec 560 at the demultiplexing part 558 during an image pick-up with CCD camera 536.

[0296]The demultiplexing part 558 multiplexes the coded image data supplied from the image encoder 554, and the voice data supplied from the voice codec 560 by a prescribed method, Spectrum diffusion treatment of the multiplexing data obtained as a result is carried out in the strange demodulator circuit unit 559, and after performing digital-to-analog conversion processing and frequency conversion processing with the transmitting and receiving circuit section 564, it transmits via the antenna 534.

[0297]On the other hand, the digital cellular phone terminal 16 with a camera, When the data of the video file linked to the simple homepage etc. is received in data communication mode, Spectrum back-diffusion-of-gas processing of the input signal received from the base station via the antenna 534 is carried out in the strange demodulator circuit unit 559, and the multiplexing data obtained as a result is sent out to the demultiplexing part 558.

[0298]The demultiplexing part 558 divides multiplexing data into coded image data and voice data, and supplies coded image data to the image decoder 557 via the synchronous bus 562, and it supplies voice data to the voice codec 560.

[0299]By decoding coded image data with the decode system corresponding to predetermined coding modes, such as MPEG 2 or MPEG4, the image decoder 557 generates reproduction dynamic image data, and supplies this to the liquid crystal display 538 via the LCD control section 556. Thereby, the digital cellular phone terminal 16 with a camera displays the video data contained in the video file linked to the simple homepage, for example.

[0300]At this time, simultaneously, the voice codec 560 supplies this to the loudspeaker 537, after changing voice data into an analog voice signal. Thereby, the digital cellular phone terminal 16 with a camera reproduces \*\*\*\*\* voice data to the video file linked to the simple homepage, for example.

[0301]Although the personal computer 1 or the digital cellular phone terminal 16 with

a camera transmitted the number of the credit card and it explained that the recognition server 3, the ID management server 8, or the locker server 11 recorded the number of a credit card, What is necessary is just the information which can process fee collection, such as a number of not only the number of a credit card but a bank account, or a registration number of an Internet connectivity service provider.

[0302]Although a series of processings mentioned above can also be performed by hardware, they can also be performed with software. The computer by which the program which constitutes the software is included in hardware for exclusive use when performing a series of processings with software, Or it is installed in the personal computer etc. which can perform various kinds of functions, for example, are general-purpose, etc. from a program storing medium by installing various kinds of programs.

[0303]The program storing medium which stores the program which is installed in a computer and it changes into the state which can be performed by computer, As shown in drawing 3 or drawing 4, the magnetic disk 91 or 131 (a floppy disk is included), the optical disc 92 or 132 (CD-ROM (Compact Disc-Read Only Memory).) . DVD (Digital Versatile Disc) is included. The package media which consist of the magneto-optical disc 93 or 133 (MD (Mini-Disc) is included) or the semiconductor memory 94 or 134, Or a program is constituted by ROM72 stored temporarily or permanently or 102, HDD81, 111, etc. Storing of the program to a program storing medium is performed via the interface of a router, a modem, etc. using the communication media of cables or radio, such as a Local Area Network, the Internet, and digital satellite broadcasting, if needed.

[0304]In this specification, even if the processing serially performed in accordance with an order that the step which describes the program stored in a program storing medium was indicated is not of course necessarily processed serially, it also includes a parallel target or the processing performed individually.

[0305]In this specification, a system expresses the whole device constituted by two or more devices.

[0306]

[Effect of the Invention]According to the information processor according to claim 1, the information processing method according to claim 4, and the program storing medium according to claim 5. When the identification data transmitted from other information processors was received and identification data is received, Since the group key shared in the group to whom other information processors belong is generated, a group key is recorded corresponding to identification data and the group key was transmitted to other information processors, Desired contents can be used with the information processor of the request belonging to a group, preventing use of the third party who does not have a just right.

[0307]According to the information processor according to claim 6, the information



processing method according to claim 8, and the program storing medium according to claim 9. ID which specifies a group is memorized, and ID which specifies a group from other information processors is received, and is memorized. Since received ID is compared and the data which recognizes the copy operation of the information was made to be outputted to other information processors based on the comparison result, Desired contents can be used with the information processor of the request belonging to a group, preventing use of the third party who does not have a just right.

[0308]According to the information processor according to claim 10, the information processing method according to claim 14, and the program storing medium according to claim 15. To other 1st information processor, identification data is transmitted and from other 1st information processor. Since the contents key which has enciphered contents was enciphered with the group key when the group key shared in a group was received, the received group key was memorized and contents were outputted, Desired contents can be used with the information processor of the request belonging to a group, preventing use of the third party who does not have a just right.

---

## DESCRIPTION OF DRAWINGS

---

[Brief Description of the Drawings]

[Drawing 1]It is a figure explaining the program which enciphers, records, decodes and uses the conventional contents.

[Drawing 2]It is a figure showing the 1 embodiment of the music data managerial system concerning this invention.

[Drawing 3]It is a figure explaining the composition of the personal computer 1-1.

[Drawing 4]It is a figure explaining the composition of the recognition server 3.

[Drawing 5]It is a block diagram explaining the composition of the function of the personal computer 1-1.

[Drawing 6]It is a figure explaining the contents which the personal computer 1 is recording.

[Drawing 7]It is a figure explaining the contents which the personal computer 1 outputs.

[Drawing 8]It is a figure explaining operation of the personal computer 1-2 which imports the contents 251.

[Drawing 9]It is a figure explaining recognition of the recognition server 3 at the time of import of contents.

[Drawing 10]It is a figure explaining the processing which registers the personal computer 1-1 belonging to one group thru/or 1-3 into the recognition server 3.

[Drawing 11]It is a figure explaining processing when importing contents.

[Drawing 12]It is a flow chart explaining processing of registration.

[Drawing 13]It is a flow chart explaining a group's ID and the example of processing of generation of a password.

[Drawing 14]It is a flow chart explaining processing of the output of contents.

[Drawing 15]It is a flow chart explaining the processing which imports contents.

[Drawing 16]It is a figure explaining other examples of a group's ID and the controlling method of a password.

[Drawing 17]It is a flow chart explaining processing of registration.

[Drawing 18]It is a flow chart explaining processing of generation of ID by the ID management server 8, and a password.

[Drawing 19]It is a flow chart explaining processing of registration by the personal computer 1 and EMD server 4.

[Drawing 20]It is a flow chart explaining processing of settlement of accounts.

[Drawing 21]It is a figure explaining other processings which import contents.

[Drawing 22]It is a flow chart explaining processing of transmission of the group key 271.

[Drawing 23]It is a figure explaining processing of the registration to the locker server 11.

[Drawing 24]It is a figure explaining the example of the list of contents which the locker server 11 is recording.

[Drawing 25]It is a figure explaining common use of the contents by the locker server 11.

[Drawing 26]It is a figure explaining common use of the contents by the locker server 11.

[Drawing 27]It is a figure explaining processing of the fee collection by the locker server 11.

[Drawing 28]It is a flow chart explaining processing of registration by the personal computer 1 and the locker server 11.

[Drawing 29]It is a flow chart explaining processing of record of the contents to the locker server 11.

[Drawing 30]It is a flow chart explaining processing of read-out of the contents from the locker server 11.

[Drawing 31]It is a figure showing a 2nd embodiment of the music data managerial system concerning this invention.

[Drawing 32]It is a figure explaining the digital cellular phone terminal 16 with a camera.

[Drawing 33]It is a figure explaining the digital cellular phone terminal 16 with a camera.

[Drawing 34]It is a figure explaining the composition of the digital cellular phone terminal 16 with a camera.

[Description of Notations]

1-1,1-2 A personal computer and 2. A network and 3 A recognition server and 8 ID-management server, 11 A locker server, 12-1 to 12-4. A portable device, 13-1 to 13-3. A memory card and a digital cellular phone terminal with 16 cameras, 51 A contents managing program and 52. A display operation instruction program and 53 A contents database, 54-1 thru/or the application program for 54-3 purchase, 61 Group gateway programs, 71 CPU, 72 ROM, and 73 RAM, 81 HDD and 85 The communications department and 91 magnetic disks, 92 An optical disc and 93 magneto-optical discs, 94 Semiconductor memory and 101 CPU, 102 ROM, 103RAM, 111 HDD, and 113 The communications department, 131 magnetic disks, 132 optical discs, 133 magneto-optical discs, 134 semiconductor memory, and 401 A contents database and 551 Main control part

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-169726

(P2002-169726A)

(43) 公開日 平成14年6月14日 (2002.6.14)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード*(参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 B 5 B 0 1 7
	3 1 0		3 1 0 K 5 J 1 0 4
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00	6 6 0 E
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 D
			6 0 1 E
審査請求 未請求 請求項の数15 O L (全 33 頁)			

(21) 出願番号 特願2000-364896(P2000-364896)

(22) 出願日 平成12年11月30日 (2000.11.30)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 實藤 隆則

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72) 発明者 河上 達

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74) 代理人 100082131

弁理士 稲本 義雄

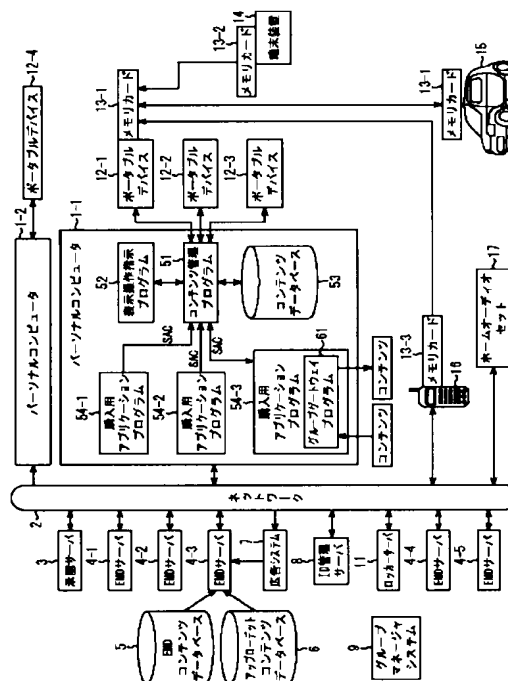
最終頁に続く

(54) 【発明の名称】 情報処理装置および方法、並びにプログラム格納媒体

(57) 【要約】

【課題】 正当な権利を有さない第三者の利用を防止しつつ、コンテンツを所望の情報処理装置で利用する。

【解決手段】 承認サーバ3は、パーソナルコンピュータ1-1から送信された、コンテンツの管理用プログラムを特定するデータを受信し、グループにおいて共用されるグループ鍵を生成し、コンテンツ管理用プログラムを特定するデータとグループ鍵とを対応させて記録し、グループ鍵をパーソナルコンピュータ1-1へ送信する。



## 【特許請求の範囲】

【請求項 1】 他の情報処理装置から送信された識別データを受信する第 1 の受信手段と、

前記識別データを受信した場合、前記他の情報処理装置が属するグループにおいて共用されるグループ鍵を生成する生成手段と、

前記グループ鍵を、前記識別データに対応して記録する記録手段と、

前記グループ鍵を、前記他の情報処理装置へ送信する第 1 の送信手段とを含むことを特徴とする情報処理装置。

【請求項 2】 前記第 1 の受信手段は、前記識別データとして、前記他の情報処理装置のコンテンツ管理用プログラムを特定するデータを受信することを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】 前記生成手段は、前記第 1 の受信手段が、同一のグループの前記他の情報処理装置から初めて前記識別データを受信した場合、前記グループを特定する ID もさらに生成することを特徴とする請求項 1 に記載の情報処理装置。

【請求項 4】 情報処理装置から送信された識別データを受信する受信ステップと、

前記識別データを受信した場合、前記情報処理装置が属するグループにおいて共用されるグループ鍵を生成する生成ステップと、

前記グループ鍵を、前記識別データに対応して記録する記録ステップと、

前記グループ鍵を、前記情報処理装置へ送信する送信ステップとを含むことを特徴とする情報処理方法。

【請求項 5】 情報処理装置から送信された識別データを受信する受信ステップと、

前記識別データを受信した場合、前記情報処理装置が属するグループにおいて共用されるグループ鍵を生成する生成ステップと、

前記グループ鍵を、前記識別データに対応して記録する記録ステップと、

前記グループ鍵を、前記情報処理装置へ送信する送信ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが格納されているプログラム格納媒体。

【請求項 6】 複数の他の情報処理装置が有する、グループにおいて共用されるグループ鍵に基づき、前記他の情報処理装置による情報のコピー動作を管理する情報処理装置において、

前記グループを特定する ID を記憶する記憶手段と、

前記他の情報処理装置から前記グループを特定する ID を受信する受信手段と、

前記記憶手段により記憶されている前記 ID と、前記受信手段により受信された前記 ID とを比較する比較手段と、

前記比較手段の比較結果に基づいて、前記他の情報処理

装置に対して、その情報のコピー動作を承認するデータを出力する出力手段とを含むことを特徴とする情報処理装置。

【請求項 7】 前記記憶手段は、さらにパスワードを記憶し、

前記受信手段は、前記パスワードをさらに受信し、

前記比較手段は、前記 ID とパスワードを比較することとを特徴とする請求項 6 に記載の情報処理装置。

【請求項 8】 複数の情報処理装置が有する、グループにおいて共用されるグループ鍵に基づき、前記情報処理装置による情報のコピー動作を管理する情報処理方法において、

前記グループを特定する ID を記憶する記憶ステップと、

前記情報処理装置から前記グループを特定する ID を受信する受信ステップと、

前記記憶ステップの処理により記憶されている前記 ID と、前記受信ステップの処理により受信された前記 ID とを比較する比較ステップと、

前記比較ステップの処理の比較結果に基づいて、前記情報処理装置に対して、その情報のコピー動作を承認するデータを出力する出力ステップとを含むことを特徴とする情報処理方法。

【請求項 9】 複数の情報処理装置が有する、グループにおいて共用されるグループ鍵に基づき、前記情報処理装置による情報のコピー動作を管理する情報処理用のプログラムであって、

前記グループを特定する ID を記憶する記憶ステップと、

前記情報処理装置から前記グループを特定する ID を受信する受信ステップと、

前記記憶ステップの処理により記憶されている前記 ID と、前記受信ステップの処理により受信された前記 ID とを比較する比較ステップと、

前記比較ステップの処理の比較結果に基づいて、前記情報処理装置に対して、その情報のコピー動作を承認するデータを出力する出力ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが格納されているプログラム格納媒体。

【請求項 10】 第 1 の他の情報処理装置に対して、識別データを送信する第 1 の送信手段と、

前記第 1 の他の情報処理装置から、グループにおいて共用されるグループ鍵を受信する第 1 の受信手段と、

前記第 1 の受信手段により受信された前記グループ鍵を記憶する記憶手段と、コンテンツを出力する場合、前記コンテンツを暗号化しているコンテンツ鍵を前記グループ鍵で暗号化する暗号化手段とを含むことを特徴とする情報処理装置。

【請求項 11】 前記コンテンツ鍵を復号する復号手段をさらに含み、

前記暗号化手段は、前記復号手段により復号された前記コンテンツ鍵を暗号化することを特徴とする請求項10に記載の情報処理装置。

【請求項12】 前記グループを特定するIDとパスワードを取得する取得手段と、

前記取得手段により取得された前記IDとパスワードを、第2の他の情報処理装置に対して送信する第2の送信手段と、

前記第2の他の情報処理装置から、前記コンテンツのコピー動作を承認するデータを受信する第2の受信手段と、

前記第2の受信手段により受信された前記コンテンツのコピー動作を承認するデータに基づいて、前記コンテンツのコピー動作を制御するコピー制御手段とをさらに含むことを特徴とする請求項10に記載の情報処理装置。

【請求項13】 前記第1の送信手段は、前記識別データとして、前記情報処理装置のコンテンツ管理用プログラムを特定するデータを送信することを特徴とする請求項10に記載の情報処理装置。

【請求項14】 情報処理装置に対して、識別データを送信する送信ステップと、

前記情報処理装置から、グループにおいて共用されるグループ鍵を受信する受信ステップと、

前記受信ステップの処理により受信された前記グループ鍵を記憶する記憶ステップと、

コンテンツを出力する場合、前記コンテンツを暗号化しているコンテンツ鍵を前記グループ鍵で暗号化する暗号化ステップとを含むことを特徴とする情報処理方法。

【請求項15】 情報処理装置に対して、識別データを送信する送信ステップと、

前記情報処理装置から、グループにおいて共用されるグループ鍵を受信する受信ステップと、

前記受信ステップの処理により受信された前記グループ鍵を記憶する記憶ステップと、

コンテンツを出力する場合、前記コンテンツを暗号化しているコンテンツ鍵を前記グループ鍵で暗号化する暗号化ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが格納されているプログラム格納媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報処理装置および方法、並びにプログラム格納媒体に関し、特に、不正なコンテンツの利用を防止する情報処理装置および方法、並びにプログラム格納媒体に関する。

【0002】

【従来の技術】音楽、画像などのコンテンツを暗号化することによりコンテンツの不正な使用を防止する技術が利用されている。

【0003】図1は、従来のコンテンツを暗号化して記

録し、再生するとき復号するプログラムを説明する図である。秘置プログラムは、使用者により入力されたIDおよびパスワードを基に、暗号化鍵を生成して、生成した暗号化鍵でコンテンツを暗号化する。

【0004】暗号化されていコンテンツを再生するとき、解読プログラムは、使用者にIDおよびパスワードの入力を要求し、正しいIDおよびパスワードが入力されたとき、IDおよびパスワードを基に、復号鍵を生成して、復号鍵でコンテンツを復号する。

【0005】このようにすることで、正しいIDおよびパスワードを知らなければ、コンテンツを利用することはできず、コンテンツの不正な利用を防止することができる。

【0006】また、復号鍵をストレージ鍵で暗号化し、コンテンツを利用する機器にストレージ鍵をセキュアに記憶させる技術も利用されている。

【0007】

【発明が解決しようとする課題】しかしながら、復号鍵をストレージ鍵で暗号化し、ストレージ鍵をセキュアに記憶している機器でコンテンツを利用するとき、複数の機器を所有している利用者は、所定の機器でのみ所定のコンテンツを利用することができ、所望のコンテンツを所望の機器で利用することができないという問題点があった。

【0008】本発明はこのような状況に鑑みてなされたものであり、正当な権利を有さない第三者の利用を防止しつつ、所望のコンテンツを所望の機器で利用することができるようにすることを目的とする。

【0009】

30 【課題を解決するための手段】請求項1に記載の情報処理装置は、他の情報処理装置から送信された識別データを受信する第1の受信手段と、識別データを受信した場合、他の情報処理装置が属するグループにおいて共用されるグループ鍵を生成する生成手段と、グループ鍵を、識別データに対応して記録する記録手段と、グループ鍵を、他の情報処理装置へ送信する第1の送信手段とを含むことを特徴とする。

40 【0010】第1の受信手段は、識別データとして、他の情報処理装置のコンテンツ管理用プログラムを特定するデータを受信するようにすることができる。

【0011】生成手段は、第1の受信手段が、同一のグループの他の情報処理装置から初めて識別データを受信した場合、グループを特定するIDもさらに生成するようにすることができる。

【0012】請求項4に記載の情報処理方法は、情報処理装置から送信された識別データを受信する受信ステップと、識別データを受信した場合、情報処理装置が属するグループにおいて共用されるグループ鍵を生成する生成ステップと、グループ鍵を、識別データに対応して記録する記録ステップと、グループ鍵を、情報処理装置へ

送信する送信ステップとを含むことを特徴とする。

【0013】請求項5に記載のプログラム格納媒体のプログラムは、情報処理装置から送信された識別データを受信する受信ステップと、識別データを受信した場合、情報処理装置が属するグループにおいて共用されるグループ鍵を生成する生成ステップと、グループ鍵を、識別データに対応して記録する記録ステップと、グループ鍵を、情報処理装置へ送信する送信ステップとを含むことを特徴とする。

【0014】請求項6に記載の情報処理装置は、グループを特定するIDを記憶する記憶手段と、他の情報処理装置からグループを特定するIDを受信する受信手段と、記憶手段により記憶されているIDと、受信手段により受信されたIDとを比較する比較手段と、比較手段の比較結果に基づいて、他の情報処理装置に対して、その情報のコピー動作を承認するデータを出力する出力手段とを含むことを特徴とする。

【0015】記憶手段は、さらにパスワードを記憶し、受信手段は、パスワードをさらに受信し、比較手段は、IDとパスワードを比較するようにすることができる。

【0016】請求項8に記載の情報処理方法は、グループを特定するIDを記憶する記憶ステップと、情報処理装置からグループを特定するIDを受信する受信ステップと、記憶ステップの処理により記憶されているIDと、受信ステップの処理により受信されたIDとを比較する比較ステップと、比較ステップの処理の比較結果に基づいて、情報処理装置に対して、その情報のコピー動作を承認するデータを出力する出力ステップとを含むことを特徴とする。

【0017】請求項9に記載のプログラム格納媒体のプログラムは、グループを特定するIDを記憶する記憶ステップと、情報処理装置からグループを特定するIDを受信する受信ステップと、記憶ステップの処理により記憶されているIDと、受信ステップの処理により受信されたIDとを比較する比較ステップと、比較ステップの処理の比較結果に基づいて、情報処理装置に対して、その情報のコピー動作を承認するデータを出力する出力ステップとを含むことを特徴とする。

【0018】請求項10に記載の情報処理装置は、第1の他の情報処理装置に対して、識別データを送信する第1の送信手段と、第1の他の情報処理装置から、グループにおいて共用されるグループ鍵を受信する第1の受信手段と、第1の受信手段により受信されたグループ鍵を記憶する記憶手段と、コンテンツを出力する場合、コンテンツを暗号化しているコンテンツ鍵をグループ鍵で暗号化する暗号化手段とを含むことを特徴とする。

【0019】情報処理装置は、コンテンツ鍵を復号する復号手段をさらに設け、暗号化手段は、復号手段により復号されたコンテンツ鍵を暗号化するようにすることができる。

【0020】情報処理装置は、グループを特定するIDとパスワードを取得する取得手段と、取得手段により取得されたIDとパスワードを、第2の他の情報処理装置に対して送信する第2の送信手段と、第2の他の情報処理装置から、コンテンツのコピー動作を承認するデータを受信する第2の受信手段と、第2の受信手段により受信されたコンテンツのコピー動作を承認するデータに基づいて、コンテンツのコピー動作を制御するコピー制御手段とを更に設けることができる。

10 【0021】第1の送信手段は、識別データとして、情報処理装置のコンテンツ管理用プログラムを特定するデータを送信するようにすることができる。

【0022】請求項14に記載の情報処理方法は、情報処理装置に対して、識別データを送信する送信ステップと、情報処理装置から、グループにおいて共用されるグループ鍵を受信する受信ステップと、受信ステップの処理により受信されたグループ鍵を記憶する記憶ステップと、コンテンツを出力する場合、コンテンツを暗号化しているコンテンツ鍵をグループ鍵で暗号化する暗号化ステップとを含むことを特徴とする。

20 【0023】請求項15に記載のプログラム格納媒体のプログラムは、情報処理装置に対して、識別データを送信する送信ステップと、情報処理装置から、グループにおいて共用されるグループ鍵を受信する受信ステップと、受信ステップの処理により受信されたグループ鍵を記憶する記憶ステップと、コンテンツを出力する場合、コンテンツを暗号化しているコンテンツ鍵をグループ鍵で暗号化する暗号化ステップとを含むことを特徴とする。

30 【0024】請求項1に記載の情報処理装置、請求項4に記載の情報処理方法、および請求項5に記載のプログラム格納媒体においては、他の情報処理装置から送信された識別データが受信され、識別データを受信した場合、他の情報処理装置が属するグループにおいて共用されるグループ鍵が生成され、グループ鍵が、識別データに対応して記録され、グループ鍵が、他の情報処理装置へ送信される。

40 【0025】請求項6に記載の情報処理装置、請求項8に記載の情報処理方法、および請求項9に記載のプログラム格納媒体においては、グループを特定するIDが記憶され、他の情報処理装置からグループを特定するIDが受信され、記憶されているIDと、受信されたIDとが比較され、比較結果に基づいて、他の情報処理装置に対して、その情報のコピー動作を承認するデータが出力される。

50 【0026】請求項10に記載の情報処理装置、請求項14に記載の情報処理方法、および請求項15に記載のプログラム格納媒体においては、第1の他の情報処理装置に対して、識別データが送信され、第1の他の情報処理装置から、グループにおいて共用されるグループ鍵が

受信され、受信されたグループ鍵が記憶され、コンテンツを出力する場合、コンテンツを暗号化しているコンテンツ鍵がグループ鍵で暗号化される。

【0027】

【発明の実施の形態】図2は、本発明に係る音楽データ管理システムの一実施の形態を示す図である。パーソナルコンピュータ1-1は、ローカルエリアネットワークまたはインターネットなどから構成されるネットワーク2に接続されている。

【0028】パーソナルコンピュータ1-1は、コンテンツ管理プログラム51、表示操作指示プログラム52、および購入用アプリケーションプログラム54-1乃至54-3を実行すると共に、その内部にコンテンツデータベース53を構成する。

【0029】コンテンツ管理プログラム51は、詳細は後述するが、コンテンツを暗号化してコンテンツデータベース53に記録させると共に、暗号化されてコンテンツデータベース53に記録されているコンテンツの利用を管理する。

【0030】表示操作指示プログラム52は、コンテンツに関する情報を表示するとともに、入力された操作に対応する指示、例えば、コンテンツの再生、またはコンテンツのインポートなどの指示をコンテンツ管理プログラム51に与える。

【0031】コンテンツデータベース53は、コンテンツ管理プログラム51から供給された暗号化されているコンテンツを記録すると共に、コンテンツ管理プログラム51の要求に対応して暗号化されているコンテンツをコンテンツ管理プログラム51に供給する。

【0032】購入用アプリケーションプログラム54-1乃至54-3は、EMDサーバ4-1乃至4-3からのコンテンツの購入の処理を実行する。購入用アプリケーションプログラム54-1乃至54-3は、コンテンツ管理プログラム51と、SAC(Secure Authentication Channel)で結合されている。

【0033】購入用アプリケーションプログラム54-3は、グループゲートウェイプログラム61を実行する。グループゲートウェイプログラム61は、暗号化されているコンテンツを外部に出力するとき、コンテンツを復号するためのコンテンツ鍵を後述するグループ鍵で暗号化し、許可されている機器でのみコンテンツを利用できるようにする。グループゲートウェイプログラム61は、暗号化されているコンテンツをインポートするとき、コンテンツを復号するためのコンテンツ鍵を後述するグループ鍵で復号する。インポートとは、コンテンツを利用可能な状態で記録することをいう。

【0034】パーソナルコンピュータ1-1およびパーソナルコンピュータ1-2は、ネットワーク2を介して、使用者のクレジットカードの番号を承認サーバ3に送信して、承認サーバ3に登録し、承認サーバ3から後

述するグループ鍵、ID、およびパスワードを取得する。

【0035】承認サーバ3は、パーソナルコンピュータ1-1に登録したとき、パーソナルコンピュータ1-1の使用者のクレジットカードの番号、ID、およびパスワードをID管理サーバ8に記録させる。承認サーバ3は、例えば、パーソナルコンピュータ1-1から出力されたコンテンツをパーソナルコンピュータ1-2がインポートするとき、パーソナルコンピュータ1-2を承認する。

【0036】パーソナルコンピュータ1-2は、承認サーバ3から承認されないとき、パーソナルコンピュータ1-1から出力されたコンテンツをインポートすることができない。

【0037】パーソナルコンピュータ1-1は、EMD(Electrical Music Distribution)サーバ4-1乃至4-3から受信した、または後述するCD(Compact Disc)から読み取った音楽のデータ(以下、コンテンツと称する)を、所定の圧縮の方式(例えば、ATRAC3(商標))に変換するとともにDES(Data Encryption Standard)などの暗号化方式で暗号化して記録する。

【0038】パーソナルコンピュータ1-1は、暗号化して記録しているコンテンツに対応して、コンテンツの利用条件を示す利用条件のデータを記録する。利用条件のデータは、例えば、その利用条件のデータに対応するコンテンツを同時に3台のポータブルデバイス(Portable Device(PDとも称する))12-1乃至12-3で利用できる、コピーすることができる、他のパーソナルコンピュータに移動することができるなどを示す。

【0039】パーソナルコンピュータ1-1は、暗号化して記録しているコンテンツを、コンテンツに関連するデータ(例えば、曲名、再生回数、再生期限、またはイコライザ情報など)と共に、接続されているポータブルデバイス12-1に記憶させるとともに、ポータブルデバイス12-1に記憶させたことに対応して、記憶させたコンテンツに対応する利用条件のデータを更新する(以下、チェックアウトと称する)。パーソナルコンピュータ1-1は、暗号化して記録しているコンテンツを、コンテンツに関連するデータと共に、接続されているポータブルデバイス12-2に記憶させるとともに、ポータブルデバイス12-2に記憶させたことに対応して、記憶させたコンテンツに対応する利用条件のデータを更新する。パーソナルコンピュータ1-1は、暗号化して記録しているコンテンツを、コンテンツに関連するデータと共に、接続されているポータブルデバイス12-3に記憶させるとともに、ポータブルデバイス12-3に記憶させたことに対応して、記憶させたコンテンツに対応する利用条件のデータを更新する。

【0040】また、パーソナルコンピュータ1-1は、接続されているポータブルデバイス12-1にパーソナルコンピュータ1-1がチェックアウトしたコンテンツ



を、ポータブルデバイス12-1に消去させて、消去させたコンテンツに対応する利用条件のデータを更新する（以下、チェックインと称する）。パーソナルコンピュータ1-1は、接続されているポータブルデバイス12-2にパーソナルコンピュータ1-1がチェックアウトしたコンテンツを、ポータブルデバイス12-2に消去させて、消去させたコンテンツに対応する利用条件のデータを更新する。パーソナルコンピュータ1-1は、接続されているポータブルデバイス12-3にパーソナルコンピュータ1-1がチェックアウトしたコンテンツを、ポータブルデバイス12-3に消去させて、消去させたコンテンツに対応する利用条件のデータを更新する。

【0041】パーソナルコンピュータ1-1は、パーソナルコンピュータ1-2がポータブルデバイス12-1にチェックアウトしたコンテンツをチェックインできない。パーソナルコンピュータ1-1は、パーソナルコンピュータ1-2がポータブルデバイス12-2にチェックアウトしたコンテンツをチェックインできない。パーソナルコンピュータ1-1は、パーソナルコンピュータ1-2がポータブルデバイス12-3にチェックアウトしたコンテンツをチェックインできない。

【0042】パーソナルコンピュータ1-2は、ローカルエリアネットワークまたはインターネットなどから構成されるネットワーク2に接続されている。パーソナルコンピュータ1-2は、EMDサーバ4-1乃至4-3から受信した、または後述するCDから読み取ったコンテンツを、所定の圧縮の方式に変換するとともにDESなどの暗号化方式で暗号化して記録する。

【0043】パーソナルコンピュータ1-2は、暗号化して記録しているコンテンツに対応して、コンテンツの利用条件を示す利用条件のデータを記録する。利用条件のデータは、例えば、その利用条件のデータに対応するコンテンツを同時に3台のポータブルデバイスで利用できる、コピーすることができる、他のパーソナルコンピュータに移動することができるなどを示す。

【0044】パーソナルコンピュータ1-2は、暗号化して記録しているコンテンツを、コンテンツに関連するデータと共に、接続されているポータブルデバイス12-4に記憶させるとともに、ポータブルデバイス12-4に記憶させたことに対応して、記憶させたコンテンツに対応する利用条件のデータを更新する（すなわち、チェックアウトする）。コンテンツのチェックアウトの指示があった場合、パーソナルコンピュータ1-2は、そのコンテンツに後述する使用期限または再生回数などが設定されているとき、そのコンテンツをポータブルデバイス12-4にチェックアウトしない。

【0045】また、パーソナルコンピュータ1-2は、接続されているポータブルデバイス12-4にパーソナルコンピュータ1-2がチェックアウトしたコンテンツ

を、ポータブルデバイス12-4に消去させて、消去させたコンテンツに対応する利用条件のデータを更新する。

【0046】パーソナルコンピュータ1-2は、パーソナルコンピュータ1-1がポータブルデバイス12-4にチェックアウトしたコンテンツをチェックインできない。

【0047】以下、パーソナルコンピュータ1-1およびパーソナルコンピュータ1-2を個々に区別する必要がないとき、単にパーソナルコンピュータ1と称する。

【0048】EMDサーバ4-1は、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、コンテンツに関連するデータと共に、パーソナルコンピュータ1にコンテンツを供給する。EMDサーバ4-2は、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、コンテンツに関連するデータと共に、パーソナルコンピュータ1にコンテンツを供給する。

【0049】EMDサーバ4-3は、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、コンテンツに関連するデータ（例えば、曲名、再生回数、再生期限、またはイコライザ情報など）と共に、EMDコンテンツデータベース5から供給されたコンテンツ、またはアップロードコンテンツデータベース6から供給されたコンテンツを、パーソナルコンピュータ1に供給する。EMDサーバ4-1は、ネットワーク2を介して、広告システム7から供給された広告用データをパーソナルコンピュータ1-1またはパーソナルコンピュータ1-2に供給する。

【0050】EMDサーバ4-1乃至4-3のそれぞれが供給するコンテンツは、同一または異なる圧縮の方式で圧縮されている。EMDサーバ4-1乃至4-3のそれぞれが供給するコンテンツは、同一または異なる暗号化の方式で暗号化されている。

【0051】使用者がEMDサーバ4-1乃至4-5のいずれかからコンテンツを購入するとき、ID管理サーバ8は、パーソナルコンピュータ1-1の登録により、記録されたパーソナルコンピュータ1-1の使用者のクレジットカードの番号、ID、およびパスワードを、コンテンツが購入されるEMDサーバ4-1乃至4-5のいずれかに送信する。EMDサーバ4-1乃至4-5は、コンテンツを販売したとき、ID管理サーバ8から供給されたクレジットカードの番号、ID、およびパスワードを基に、課金の処理を実行する。

【0052】グループマネージャシステム9は、承認サーバ3の登録、またはコンテンツの利用の承認、およびID管理サーバ8のクレジットカードの番号、ID、およびパスワードの記録または送信など、コンテンツ、ID、およびパスワードの利用条件などを管理する。

【0053】ロッカーサーバ11は、ネットワーク2を

介して、パーソナルコンピュータ1-1またはパーソナルコンピュータ1-2から供給されたコンテンツを記録し、コンテンツの送信要求に対応して、記録されているコンテンツをパーソナルコンピュータ1-1またはパーソナルコンピュータ1-2に送信する。

【0054】ポータブルデバイス12-1は、パーソナルコンピュータ1から供給されたコンテンツ（すなわち、チェックアウトされたコンテンツ）を、コンテンツに関連するデータ（例えば、曲名、再生回数、再生期限、またはイコライザ情報など）と共に装着されているメモリカード13-1に記憶させる。ポータブルデバイス12-1は、コンテンツに関連するデータに基づいて、メモリカード13-1に記憶しているコンテンツを再生し、図示せぬヘッドフォンなどに出力する。

【0055】例えば、コンテンツに関連するデータとして記憶されている再生回数を超えて再生しようとしたとき、ポータブルデバイス12-1は、対応するコンテンツの再生を停止する。コンテンツに関連するデータとして記憶されている再生期限を過ぎた後に再生しようとしたとき、ポータブルデバイス12-1は、対応するコンテンツの再生を停止する。ポータブルデバイス12-1は、コンテンツに関連するデータとして記憶されているイコライザ情報を基に、音声をイコライジングして、出力する。

【0056】使用者は、ポータブルデバイス12-1をパーソナルコンピュータ1から取り外して、持ち歩き、メモリカード13-1に記憶しているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

【0057】また、ポータブルデバイス12-1は、店頭などに設置されている端末装置14により供給されたコンテンツを記憶しているメモリカード13-2を装着することにより、メモリカード13-2に記憶されているコンテンツを再生することができる。

【0058】ポータブルデバイス12-1を介してコンテンツが記憶されたメモリカード13-1は、ポータブルデバイス12-1から取り外されて、自動車15のオーディオセットに装着される。メモリカード13-1が装着された自動車15のオーディオセットは、メモリカード13-1に記憶されているコンテンツを読み出して、コンテンツを再生する。

【0059】メモリカード13-3が装着されているカメラ付きデジタル携帯電話機16は、ネットワーク2を介して、EMDサーバ4-4にコンテンツの供給を要求し、EMDサーバ4-4から供給されたコンテンツをメモリカード13-3に記憶させる。カメラ付きデジタル携帯電話機16は、装着されているメモリカード13-3に記憶されているコンテンツを再生する。ポータブルデバイス12-1は、コンテンツを記憶しているメモリカード13-3を装着することにより、メモリカード1

3-3に記憶されているコンテンツを再生することができる。

【0060】ポータブルデバイス12-2は、パーソナルコンピュータ1から供給されたコンテンツを、コンテンツに関連するデータと共に記憶する。ポータブルデバイス12-2は、コンテンツに関連するデータに基づいて、記憶しているコンテンツを再生し、図示せぬヘッドフォンなどに出力する。使用者は、コンテンツを記憶したポータブルデバイス12-2をパーソナルコンピュータ1から取り外して、持ち歩き、記憶しているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

【0061】ポータブルデバイス12-3は、パーソナルコンピュータ1から供給されたコンテンツを、コンテンツに関連するデータと共に記憶する。ポータブルデバイス12-3は、コンテンツに関連するデータに基づいて、記憶しているコンテンツを再生し、図示せぬヘッドフォンなどに出力する。使用者は、コンテンツを記憶したポータブルデバイス12-3をパーソナルコンピュータ1から取り外して、持ち歩き、記憶しているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

【0062】ポータブルデバイス12-4は、パーソナルコンピュータ1から供給されたコンテンツ（後述する使用期限または再生回数などが設定されていないコンテンツに限る）を、コンテンツに関連するデータと共に記憶する。ポータブルデバイス12-4は、コンテンツに関連するデータに基づいて、記憶しているコンテンツを再生し、図示せぬヘッドフォンなどに出力する。使用者は、コンテンツを記憶したポータブルデバイス12-4をパーソナルコンピュータ1から取り外して、持ち歩き、記憶しているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

【0063】ホームオーディオセット17は、ネットワーク2を介して、EMDサーバ4-5にコンテンツの供給を要求し、EMDサーバ4-5から供給されたコンテンツを記憶し、記憶されたコンテンツを再生する。

【0064】図3は、パーソナルコンピュータ1-1の構成を説明する図である。CPU（Central Processing Unit）71は、コンテンツ管理プログラム51またはグループゲートウェイプログラム61などのアプリケーションプログラムや、OS（Operating System）を実際に実行する。ROM（Read-only Memory）72は、一般的には、CPU71が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。RAM（Random-Access Memory）73は、CPU71の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。これらはCPUバスなどから構成されるホストバス74により相互に接続さ

れている。

【0065】ホストバス74は、ブリッジ75を介して、P C I (Peripheral Component Interconnect/Interface)バスなどの外部バス76に接続されている。

【0066】キーボード78は、C P U 7 1に各種の指令を入力するとき、使用者により操作される。マウス79は、ディスプレイ80の画面上のポイントの指示や選択を行うとき、使用者により操作される。ディスプレイ80は、液晶表示装置またはC R T (Cathode Ray Tube) などから成り、各種情報をテキストやイメージで表示する。H D D (Hard Disk Drive) 81は、ハードディスクを駆動し、それらにC P U 7 1によって実行するプログラムや情報を記録または再生させる。

【0067】ドライブ82は、装着されている磁気ディスク91、光ディスク92 (C Dを含む)、光磁気ディスク93、または半導体メモリ94に記録されているデータまたはプログラムを読み出して、そのデータまたはプログラムを、インターフェース77、外部バス76、ブリッジ75、およびホストバス74を介して接続されているR A M 7 3に供給する。

【0068】U S B (Universal Serial Bus) ポート83-1には、所定のケーブルを介して、ポータブルデバイス12-1が接続される。U S Bポート83-1は、インターフェース77、外部バス76、ブリッジ75、またはホストバス74を介して、H D D 81、C P U 7 1、またはR A M 7 3から供給されたデータ (例えば、コンテンツまたはポータブルデバイス12-1のコマンドなどを含む) をポータブルデバイス12-1に出力する。

【0069】U S Bポート83-2には、所定のケーブルを介して、ポータブルデバイス12-2が接続される。U S Bポート83-2は、インターフェース77、外部バス76、ブリッジ75、またはホストバス74を介して、H D D 81、C P U 7 1、またはR A M 7 3から供給されたデータ (例えば、コンテンツまたはポータブルデバイス12-2のコマンドなどを含む) をポータブルデバイス12-2に出力する。

【0070】U S Bポート83-3には、所定のケーブルを介して、ポータブルデバイス12-3が接続される。U S Bポート83-3は、インターフェース77、外部バス76、ブリッジ75、またはホストバス74を介して、H D D 81、C P U 7 1、またはR A M 7 3から供給されたデータ (例えば、コンテンツまたはポータブルデバイス12-3のコマンドなどを含む) をポータブルデバイス12-3に出力する。

【0071】スピーカ24は、インターフェース77から供給されたデータ、または、音声信号を基に、コンテンツに対応する所定の音声を出力する。

【0072】これらのキーボード78乃至スピーカ84は、インターフェース77に接続されており、インター

フェース77は、外部バス76、ブリッジ75、およびホストバス74を介してC P U 7 1に接続されている。

【0073】通信部85は、ネットワーク2が接続され、C P U 7 1、またはH D D 81から供給されたデータ (例えば、登録の要求、またはコンテンツの送信要求など) を、所定の方式のパケットに格納して、ネットワーク2を介して、送信するとともに、ネットワーク2を介して、受信したパケットに格納されているデータ (例えば、認証鍵、またはコンテンツなど) をC P U 7 1、R A M 7 3、またはH D D 81に出力する。

【0074】通信部85は、外部バス76、ブリッジ75、およびホストバス74を介してC P U 7 1に接続されている。

【0075】パーソナルコンピュータ1-2の構成は、パーソナルコンピュータ1-1の構成と同様であるので、その説明は省略する。

【0076】図4は、承認サーバ3の構成を説明する図である。C P U 1 0 1は、W e bサーバプログラムなどのアプリケーションプログラムや、O Sを実際に行う。R O M 1 0 2は、一般的には、C P U 1 0 1が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。R A M 1 0 3は、C P U 1 0 1の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。これらはC P Uバスなどから構成されるホストバス104により相互に接続されている。

【0077】ホストバス104は、ブリッジ105を介して、P C Iバスなどの外部バス106に接続されている。

【0078】キーボード108は、C P U 1 0 1に各種の指令を入力するとき、使用者により操作される。マウス109は、ディスプレイ110の画面上のポイントの指示や選択を行うとき、使用者により操作される。ディスプレイ110は、液晶表示装置またはC R Tなどから成り、各種情報をテキストやイメージで表示する。H D D 1 1 1は、ハードディスクを駆動し、それらにC P U 1 0 1によって実行するプログラムや情報を記録または再生させる。

【0079】ドライブ112は、装着されている磁気ディスク131、光ディスク132、光磁気ディスク133、または半導体メモリ134に記録されているデータまたはプログラムを読み出して、そのデータまたはプログラムを、インターフェース107、外部バス106、ブリッジ105、およびホストバス104を介して接続されているR A M 1 0 3に供給する。

【0080】これらのキーボード108乃至ドライブ112は、インターフェース107に接続されており、インターフェース107は、外部バス106、ブリッジ105、およびホストバス104を介してC P U 1 0 1に接続されている。

【0081】通信部113は、ネットワーク2が接続され、ネットワーク2を介して、受信したパケットに格納されているデータ（例えば、後述する登録に必要なデータ、または所定のプログラムのID（Identifier）など）をCPU101、RAM103、またはHDD111に出力するとともに、CPU101、またはHDD111から供給されたデータ（例えば、ID、またはパスワードなど）を、所定の方式のパケットに格納して、ネットワーク2を介して、送信する。

【0082】通信部113は、外部バス106、ブリッジ105、およびホストバス104を介してCPU101に接続されている。

【0083】EMDサーバ4-1乃至4-5、ID管理サーバ8、並びにロッカーサーバ11のそれぞれの構成は、承認サーバ3の構成と同様なので、その説明は省略する。

【0084】次に、パーソナルコンピュータ1-1が所定のプログラムを実行することにより実現する機能について説明する。

【0085】図5は、CPU71の所定のプログラムの実行等により実現される、パーソナルコンピュータ1-1の機能の構成を説明するブロック図である。

【0086】コンテンツ管理プログラム51は、EMD選択プログラム171、チェックイン／チェックアウト管理プログラム172、暗号方式変換プログラム173、圧縮方式変換プログラム174、暗号化プログラム175、利用条件変換プログラム176、署名管理プログラム177、認証プログラム178、復号プログラム179、およびPD用ドライバ180などの複数のプログラムで構成されている。

【0087】コンテンツ管理プログラム51は、例えば、シャッフルされているインストラクション、または暗号化されているインストラクションなどで記述されて、その処理内容を外部から隠蔽し、その処理内容の読解が困難になる（例えば、使用者が、直接、コンテンツ管理プログラム51を読み出しても、インストラクションを特定できないなど）ように構成されている。

【0088】EMD選択プログラム171は、コンテンツ管理プログラム51がパーソナルコンピュータ1にインストールされるとき、コンテンツ管理プログラム51には含まれず、EMDの登録の処理において、ネットワーク2を介して、図示せぬ登録サーバから受信される。EMD選択プログラム171は、EMDサーバ4-1乃至4-3のいずれかとの接続を選択して、購入用アプリケーション54-1乃至54-3に、EMDサーバ4-1乃至4-3のいずれかとの通信（例えば、コンテンツを購入するときの、コンテンツのダウンロードなど）を実行させる。

【0089】チェックイン／チェックアウト管理プログラム172は、チェックインまたはチェックアウトの設

定、およびコンテンツデータベース53に記録されている利用条件ファイル202-1乃至202-Nに基づいて、コンテンツファイル201-1乃至201-Nに格納されているコンテンツをポータブルデバイス12-1乃至12-3のいずれかにチェックアウトするか、またはポータブルデバイス12-1乃至12-3に記憶されているコンテンツをチェックインする。

【0090】チェックイン／チェックアウト管理プログラム172は、チェックインまたはチェックアウトの処理に対応して、コンテンツデータベース53に記録されている利用条件ファイル202-1乃至202-Nに格納されている利用条件のデータを更新する。

【0091】暗号方式変換プログラム173は、ネットワーク2を介して、購入用アプリケーションプログラム54-1がEMDサーバ4-1から受信したコンテンツの暗号化の方式、購入用アプリケーションプログラム54-2がEMDサーバ4-2から受信したコンテンツの暗号化の方式、または購入用アプリケーションプログラム54-3がEMDサーバ4-3から受信したコンテンツの暗号化の方式を、コンテンツデータベース53が記録しているコンテンツファイル201-1乃至201-Nに格納されているコンテンツと同一の暗号化の方式に変換する。

【0092】また、暗号方式変換プログラム173は、ポータブルデバイス12-1または12-3にコンテンツをチェックアウトするとき、チェックアウトするコンテンツを、ポータブルデバイス12-1または12-3が利用可能な暗号化方式に変換する。

【0093】圧縮方式変換プログラム174は、ネットワーク2を介して、購入用アプリケーションプログラム54-1がEMDサーバ4-1から受信したコンテンツの圧縮の方式、購入用アプリケーションプログラム54-2がEMDサーバ4-2から受信したコンテンツの圧縮の方式、または購入用アプリケーションプログラム54-3がEMDサーバ4-3から受信したコンテンツの圧縮の方式を、コンテンツデータベース53が記録しているコンテンツファイル201-1乃至201-Nに格納されているコンテンツと同一の圧縮の方式に変換する。

【0094】圧縮方式変換プログラム174は、例えばCDから読み取られ、録音プログラム151から供給されたコンテンツ（圧縮されていない）を、コンテンツデータベース53が記録しているコンテンツファイル201-1乃至201-Nに格納されているコンテンツと同一の符号化の方式で符号化する。

【0095】また、圧縮方式変換プログラム174は、ポータブルデバイス12-1または12-3にコンテンツをチェックアウトするとき、チェックアウトするコンテンツを、ポータブルデバイス12-1または12-3が利用可能な圧縮の方式に変換する。

【0096】暗号化プログラム175は、例えばCDから読み取られ、録音プログラム151から供給されたコンテンツ（暗号化されていない）を、コンテンツデータベース53が記録しているコンテンツファイル201-1乃至201-Nに格納されているコンテンツと同一の暗号化の方式で暗号化する。

【0097】利用条件変換プログラム176は、ネットワーク2を介して、購入用アプリケーションプログラム54-1がEMDサーバ4-1から受信したコンテンツの利用条件を示すデータ（いわゆる、Usage Rule）、購入用アプリケーションプログラム54-2がEMDサーバ4-2から受信したコンテンツの利用条件を示すデータ、または購入用アプリケーションプログラム54-3がEMDサーバ4-3から受信したコンテンツの利用条件を示すデータを、コンテンツデータベース53が記録している利用条件ファイル202-1乃至202-Nに格納されている利用条件データと同一のフォーマットに変換する。

【0098】また、利用条件変換プログラム176は、ポータブルデバイス12-1または12-3にコンテンツをチェックアウトするとき、チェックアウトするコンテンツに対応する利用条件のデータを、ポータブルデバイス12-1または12-3が利用可能な利用条件のデータに変換する。

【0099】署名管理プログラム177は、チェックインまたはチェックアウトの処理を実行する前に、コンテンツデータベース53に記録されている利用条件ファイル202-1乃至202-Nに格納されている利用条件のデータに含まれている署名を基に、利用条件のデータの改竄を検出する。署名管理プログラム177は、チェックインまたはチェックアウトの処理に伴う、コンテンツデータベース53に記録されている利用条件ファイル202-1乃至202-Nに格納されている利用条件のデータを更新に対応して、利用条件のデータに含まれる署名を更新する。

【0100】認証プログラム178は、コンテンツ管理プログラム51と購入用アプリケーションプログラム54-1との相互認証の処理、コンテンツ管理プログラム51と購入用アプリケーションプログラム54-2との相互認証の処理、およびコンテンツ管理プログラム51と購入用アプリケーションプログラム54-3との相互認証の処理を実行する。また、認証プログラム178は、EMDサーバ4-1と購入用アプリケーションプログラム54-1との相互認証の処理、EMDサーバ4-2と購入用アプリケーションプログラム54-2との相互認証の処理、およびEMDサーバ4-3と購入用アプリケーションプログラム54-3との相互認証の処理で利用される認証鍵を記憶している。

【0101】認証プログラム178が相互認証の処理で利用する認証鍵は、コンテンツ管理プログラム51がパ

ーソナルコンピュータ1にインストールされたとき、認証プログラム178に記憶されておらず、表示操作指示プログラム52により登録の処理が正常に実行されたとき、図示せぬ登録サーバから供給され、認証プログラム178に記憶される。

【0102】復号プログラム179は、コンテンツデータベース53が記録しているコンテンツファイル201-1乃至201-Nに格納されているコンテンツをパーソナルコンピュータ1-1が再生するとき、コンテンツを復号する。

【0103】PD用ドライバ180は、ポータブルデバイス12-2に所定のコンテンツをチェックアウトするとき、またはポータブルデバイス12-2から所定のコンテンツをチェックインするとき、ポータブルデバイス12-2にコンテンツまたはポータブルデバイス12-2に所定の処理を実行させるコマンドを供給する。

【0104】PD用ドライバ180は、ポータブルデバイス12-1に所定のコンテンツをチェックアウトするとき、またはポータブルデバイス12-1から所定のコンテンツをチェックインするとき、デバイスドライバ152-1にコンテンツ、またはデバイスドライバ152-1に所定の処理を実行させるコマンドを供給する。

【0105】PD用ドライバ180は、ポータブルデバイス12-3に所定のコンテンツをチェックアウトするとき、またはポータブルデバイス12-3から所定のコンテンツをチェックインするとき、デバイスドライバ152-2にコンテンツ、またはデバイスドライバ152-2に所定の処理を実行させるコマンドを供給する。

【0106】表示操作指示プログラム52は、フィルタリングデータファイル221、表示データファイル222、画像ファイル223-1乃至223-K、または履歴データファイル224を基に、ディスプレイ80に所定のウィンドウの画像を表示させ、キーボード78またはマウス79への操作を基に、コンテンツ管理プログラム51にチェックインまたはチェックアウトなどの処理の実行を指示する。

【0107】フィルタリングデータファイル221は、コンテンツデータベース53に記録されているコンテンツファイル201-1乃至201-Nに格納されているコンテンツそれぞれに重み付けをするためのデータを格納して、HDD81に記録されている。

【0108】表示データファイル222は、コンテンツデータベース53に記録されているコンテンツファイル201-1乃至201-Nに格納されているコンテンツに対応するデータを格納して、HDD81に記録されている。

【0109】画像ファイル223-1乃至223-Kは、コンテンツデータベース53に記録されているコンテンツファイル201-1乃至201-Nに対応する画像、またはパッケージに対応する画像を格納して、HD

D 8 1 に記録されている。

【0110】履歴データファイル224は、コンテンツデータベース53に記録されているコンテンツファイル201-1乃至201-Nに格納されているコンテンツがチェックアウトされた回数、チェックインされた回数、その日付などの履歴データを格納して、HDD81に記録されている。

【0111】表示操作指示プログラム52は、登録の処理のとき、ネットワーク2を介して、図示せぬ登録サーバに、予め記憶しているコンテンツ管理プログラム51のIDを送信するとともに、登録サーバから認証用鍵およびEMD選択プログラム171を受信して、コンテンツ管理プログラム51に認証用鍵およびEMD選択プログラム171を供給する。

【0112】録音の指示が入力されたとき、録音プログラム151は、ドライブ82に装着された光ディスク92であるCDからコンテンツを読み出して、チェックアウト最大可能回数などのコンテンツに対応する利用条件のデータなどと共に、コンテンツ管理プログラム51に出力する。

【0113】コンテンツデータベース53は、コンテンツ管理プログラム51から供給された所定的方式で圧縮され、所定的方式で暗号化されているコンテンツを、コンテンツファイル201-1乃至201-Nのいずれかに格納する（HDD81に記録する）。コンテンツデータベース53は、コンテンツファイル201-1乃至201-Nにそれぞれ格納されているコンテンツに対応する利用条件のデータを、コンテンツが格納されているコンテンツファイル201-1乃至201-Nにそれぞれ対応する利用条件ファイル202-1乃至202-Nのいずれかに格納する（HDD81に記録する）。

【0114】コンテンツデータベース53は、コンテンツファイル201-1乃至201-Nまたは利用条件ファイル202-1乃至202-Nをレコードとして記録してもよい。

【0115】例えば、コンテンツファイル201-1に格納されているコンテンツに対応する利用条件のデータは、利用条件ファイル202-1に格納されている。コンテンツファイル201-Nに格納されているコンテンツに対応する利用条件のデータは、利用条件ファイル202-Nに格納されている。

【0116】起動プログラム117は、パーソナルコンピュータ1-1のオペレーティングシステムが動作しているとき、常に動作している、いわゆる、常駐プログラムであり、デバイスドライバ152-1からポータブルデバイス12-1がUSBポート83-1に接続された旨の信号を受信した場合、表示操作指示プログラム52が起動されていないとき、表示操作指示プログラム52を起動させる。

【0117】起動プログラム117は、デバイスドライ

バ152-2からポータブルデバイス12-3がUSBポート83-3に接続された旨の信号を受信した場合、表示操作指示プログラム52が起動されていないとき、表示操作指示プログラム52を起動させる。

【0118】以下、コンテンツファイル201-1乃至201-Nを個々に区別する必要がないとき、単に、コンテンツファイル201と称する。以下、利用条件ファイル202-1乃至202-Nを個々に区別する必要がないとき、単に、利用条件ファイル202と称する。

10 【0119】パーソナルコンピュータ1-2の機能の構成は、パーソナルコンピュータ1-1の機能の構成と同様であるので、その説明は省略する。

【0120】以下、パーソナルコンピュータ1-1および1-2を個々に区別する必要がないとき、単に、パーソナルコンピュータ1と称する。

20 【0121】図6は、パーソナルコンピュータ1が記録しているコンテンツを説明する図である。購入用アプリケーションプログラム54-1は、コンテンツ鍵で暗号化されているコンテンツを、コンテンツ鍵と共にEMDサーバ4-1から受信し、SACを介して、受信したコンテンツをコンテンツ管理プログラム51に供給する。購入用アプリケーションプログラム54-1は、セッション鍵などで暗号化されているコンテンツ鍵を復号して、コンテンツ管理プログラム51に供給する。

【0122】購入用アプリケーションプログラム54-2は、コンテンツ鍵で暗号化されているコンテンツを、コンテンツ鍵と共にEMDサーバ4-2から受信し、SACを介して、受信したコンテンツをコンテンツ管理プログラム51に供給する。購入用アプリケーションプログラム54-2は、セッション鍵などで暗号化されているコンテンツ鍵を復号して、コンテンツ管理プログラム51に供給する。

30 【0123】購入用アプリケーションプログラム54-3は、コンテンツ鍵で暗号化されているコンテンツを、コンテンツ鍵と共にEMDサーバ4-3から受信し、SACを介して、受信したコンテンツをコンテンツ管理プログラム51に供給する。購入用アプリケーションプログラム54-3は、セッション鍵などで暗号化されているコンテンツ鍵を復号して、コンテンツ管理プログラム51に供給する。

40 【0124】グループゲートウェイプログラム61は、承認サーバ3への登録の処理のとき、ネットワーク2を介して、承認サーバ3に、予め記憶しているコンテンツ管理プログラム51のIDおよびクレジットカードの番号を送信するとともに、承認サーバ3からグループ鍵、ID、およびパスワードを受信する。

【0125】コンテンツ管理プログラム51は、予めストレージ鍵253をセキュアに記憶しており、表示操作指示プログラム52からの要求に従って、ストレージ鍵253で購入用アプリケーションプログラム54-1か

ら供給されたコンテンツ鍵、購入用アプリケーションプログラム54-2から供給されたコンテンツ鍵、または購入用アプリケーションプログラム54-3から供給されたコンテンツ鍵を暗号化する。

【0126】コンテンツ管理プログラム51は、コンテンツ鍵で暗号化されているコンテンツ251およびストレージ鍵253で暗号化されているコンテンツ鍵252をコンテンツファイル201としてコンテンツデータベース53に記録させる。

【0127】図7は、パーソナルコンピュータ1が出力するコンテンツを説明する図である。購入用アプリケーションプログラム54-3のグループゲートウェイプログラム61は、コンテンツ管理プログラム51にコンテンツ251-1を要求する。

【0128】コンテンツ管理プログラム51は、コンテンツデータベース53からコンテンツ251-1およびコンテンツ鍵252を読み出す。コンテンツ管理プログラム51は、記憶しているストレージ鍵253でコンテンツ鍵252を復号して、コンテンツ鍵で暗号化されているコンテンツ251-1と共に、グループゲートウェイプログラム61に供給する。

【0129】グループゲートウェイプログラム61は、復号されたコンテンツ鍵をグループ鍵271で暗号化して、グループ鍵271で暗号化されているコンテンツ鍵272と共に、コンテンツ鍵で暗号化されているコンテンツ251-2を出力する。

【0130】パーソナルコンピュータ1から出力されたコンテンツ251-2は、コンテンツ鍵で暗号化されており、コンテンツ鍵272は、グループ鍵271で暗号化されているので、そのままではコンテンツ251-2を利用することはできない。

【0131】パーソナルコンピュータ1-1から出力されたコンテンツ251-2をインポートするパーソナルコンピュータ1-2の動作を図8を参照して説明する。

【0132】パーソナルコンピュータ1-2のグループゲートウェイプログラム61-2は、正しいIDおよびパスワードが入力され、承認サーバ3から承認を得たとき、予め記憶しているグループ鍵271-2でコンテンツ鍵272を復号する。

【0133】グループゲートウェイプログラム61-2が記憶しているグループ鍵271-2は、グループゲートウェイプログラム61-1が記憶しているグループ鍵271-1と同一である。

【0134】グループゲートウェイプログラム61-2は、復号されたコンテンツ鍵とコンテンツ鍵で暗号化されているコンテンツ251-2をコンテンツ管理プログラム51-2に供給する。

【0135】コンテンツ管理プログラム51-2は、コンテンツ鍵をストレージ鍵253-2で暗号化して、ストレージ鍵253-2で暗号化されているコンテンツ鍵

252-2と共に、コンテンツ鍵で暗号化されているコンテンツ251-3をコンテンツデータベース53-2に記録させる。

【0136】パーソナルコンピュータ1-2は、パーソナルコンピュータ1-1から出力されインポートされたコンテンツ251-3を利用するとき、ストレージ鍵51-2でコンテンツ鍵252-2を復号し、復号されたコンテンツ鍵でコンテンツ251-3を復号することで平文のコンテンツを得ることができる。

【0137】このように、同一の値を有するグループ鍵271-1または271-2を有するパーソナルコンピュータ1-1およびパーソナルコンピュータ1-2は、同一のグループに属していると称する。

【0138】同一の値を有するグループ鍵271-1または271-2は、登録のとき、承認サーバ3から供給される。

【0139】図9に示すように、パーソナルコンピュータ1-1と同一のグループに属するパーソナルコンピュータ1-2は、承認サーバ3から承認されたとき、パーソナルコンピュータ1-1から出力されたコンテンツをインポートすることができる。

【0140】しかし、パーソナルコンピュータ1-1と同一のグループに属さないパーソナルコンピュータ281は、パーソナルコンピュータ1-1から出力されたコンテンツをインポートすることができず、利用することができない。

【0141】図10は、1つのグループに属するパーソナルコンピュータ1-1乃至1-3を承認サーバ3に登録する処理を説明する図である。

【0142】1つのグループに属する1台目のパーソナルコンピュータ1-1を承認サーバ3に登録するとき、パーソナルコンピュータ1-1は、パーソナルコンピュータ1-1のコンテンツ管理プログラム51のIDと共に、クレジットカードの番号、使用者の氏名、および使用者のメールアドレスなどを承認サーバ3に送信する。承認サーバ3は、パーソナルコンピュータ1-1から受信したコンテンツ管理プログラム51のID、クレジットカードの番号、使用者の氏名、および使用者のメールアドレスなど記録することにより、パーソナルコンピュータ1-1および使用者を登録する。登録が終了したとき、承認サーバ3は、グループのIDおよびパスワードと共に、グループ鍵271をパーソナルコンピュータ1-1に送信する。パーソナルコンピュータ1-1は、承認サーバ3から受信したグループ鍵271を記憶する。

【0143】承認サーバ3が送信するグループのIDは、使用者のクレジットカードの番号である。または、承認サーバ3が送信するパスワードは、使用者のクレジットカードの番号である。

【0144】このようにすることで、グループのIDまたはパスワードを他の者に知られると使用者が不測の不

利益を被る可能性が高くなるので、グループに属するパーソナルコンピュータ1を使用する使用者は、グループのIDおよびパスワードを他の者に知らせることがない。従って、パーソナルコンピュータ1-1から出力されるコンテンツは、不正に利用されることなく、複数の機器で利用することが可能になる。

【0145】パーソナルコンピュータ1-1が属するグループに属する2台目のパーソナルコンピュータ1-2を承認サーバ3に登録するとき、パーソナルコンピュータ1-2は、パーソナルコンピュータ1-2のコンテンツ管理プログラム51のIDなどを承認サーバ3に送信する。承認サーバ3は、パーソナルコンピュータ1-2から受信したコンテンツ管理プログラム51のIDなどを記録することにより、パーソナルコンピュータ1-2に登録する。承認サーバ3は、グループ鍵271をパーソナルコンピュータ1-2に送信する。パーソナルコンピュータ1-2は、承認サーバ3から受信したグループ鍵271を記憶する。

【0146】パーソナルコンピュータ1-1が属するグループに属する3台目のパーソナルコンピュータ1-3を承認サーバ3に登録するとき、パーソナルコンピュータ1-3は、パーソナルコンピュータ1-3のコンテンツ管理プログラム51のIDなどを承認サーバ3に送信する。承認サーバ3は、パーソナルコンピュータ1-3から受信したコンテンツ管理プログラム51のIDなどを記録することにより、パーソナルコンピュータ1-3に登録する。承認サーバ3は、グループ鍵271をパーソナルコンピュータ1-3に送信する。パーソナルコンピュータ1-3は、承認サーバ3から受信したグループ鍵271を記憶する。

【0147】このように、同一のグループに属するパーソナルコンピュータ1-1乃至1-3は、同一のグループ鍵271を記憶する。

【0148】図11は、コンテンツをインポートするときの処理を説明する図である。パーソナルコンピュータ1-2は、パーソナルコンピュータ1-1から供給されたコンテンツをインポートするとき、グループのIDおよびパスワードの入力を要求すると共に、承認サーバ3に承認を要求する。

【0149】パーソナルコンピュータ1-2は、正しいグループのIDおよびパスワードが入力されたとき、承認サーバ3に承認された場合、パーソナルコンピュータ1-1から供給されたコンテンツのインポートを実行する。

【0150】次に、図12のフローチャートを参照して、グループゲートウェイプログラム61を実行するパーソナルコンピュータ1および承認サーバ3による登録の処理を説明する。

【0151】ステップS1101において、グループゲートウェイプログラム61は、キーボード78の操作な

どにより入力されたクレジットカードの番号を取得する。ステップS1102において、グループゲートウェイプログラム61は、コンテンツ管理プログラム51からIDを取得して、コンテンツ管理プログラム51のIDおよびクレジットカードの番号を、ネットワーク2を介して、承認サーバ3に送信する。

【0152】ステップS2101において、承認サーバ3は、パーソナルコンピュータ1から送信されたコンテンツ管理プログラム51のIDおよびクレジットカードの番号を受信する。ステップS2102において、承認サーバ3は、クレジットカードの番号などを基に、パーソナルコンピュータ1がグループの1台目のパーソナルコンピュータであるか否かを判定し、パーソナルコンピュータ1がグループの1台目のパーソナルコンピュータであると判定された場合、ステップS2103に進み、グループ鍵271を生成する。ステップS2104において、承認サーバ3は、たとえば、クレジットカードの番号と同一であるグループのIDまたはパスワードを生成する。

【0153】ステップS2105において、承認サーバ3は、使用者に対応するアカウントを生成し、手続きは、ステップS2106に進む。

【0154】ステップS2102において、パーソナルコンピュータ1がグループの1台目のパーソナルコンピュータでない、すなわち、2台目以降のパーソナルコンピュータであると判定された場合、グループ鍵271およびアカウントの生成の処理は不要なので、ステップS2103乃至ステップS2105の処理はスキップされ、手続きは、ステップS2106に進む。

【0155】ステップS2106において、承認サーバ3は、コンテンツ管理プログラム51のIDに登録する。ステップS2107において、承認サーバ3は、ネットワーク2を介して、グループ鍵271、グループのID、およびパスワードをパーソナルコンピュータ1に送信する。

【0156】ステップS1103において、グループゲートウェイプログラム61は、承認サーバ3から送信されたグループ鍵271、グループのID、およびパスワードを受信する。ステップS1104において、グループゲートウェイプログラム61は、グループ鍵271、グループのID、およびパスワードを記録する。ステップS1105において、グループゲートウェイプログラム61は、グループのID、およびパスワードをディスプレイ80に表示し、処理は終了する。

【0157】このように、パーソナルコンピュータ1-1は、承認サーバ3に、コンテンツ管理プログラム51のIDおよびクレジットカードの番号を送信することにより、グループ鍵271、グループのID、およびパスワードを取得することができる。一方、承認サーバ3は、パーソナルコンピュータ1の登録の際に、コンテン



ツ管理プログラム51のIDおよびクレジットカードの番号を取得し、生成したグループのID、およびパスワードと共に、取得したコンテンツ管理プログラム51のIDおよびクレジットカードの番号を記録することができる。

【0158】次に、図12のステップS2104の処理に対応するグループのIDおよびパスワードの生成の処理の例を図13のフローチャートを参照して説明する。

【0159】ステップS11において、承認サーバ3は、受信したクレジットカードの番号を取得する。ステップS12において、承認サーバ3は、グループのIDおよびパスワードを生成する。ステップS12の処理において、生成されるグループのIDおよびパスワードのいずれかは、クレジットカードの番号と同一である。

【0160】ステップS13において、承認サーバ3は、クレジットカードの番号と、グループのIDおよびパスワードを対応させて記録して、処理は終了する。

【0161】このように、承認サーバ3により生成されるグループのIDおよびパスワードのいずれかは、クレジットカードの番号と同一であるので、グループのIDおよびパスワードが他人に広く知られてしまうことが防止される。

【0162】次に、パーソナルコンピュータ1のコンテンツの出力の処理を図14のフローチャートを参照して説明する。

【0163】ステップS31において、コンテンツ管理プログラム51は、コンテンツデータベース53からコンテンツ251およびコンテンツ鍵252を読み出す。コンテンツ251は、コンテンツ鍵で暗号化されており、コンテンツ鍵252は、ストレージ鍵253で暗号化されている。

【0164】ステップS32において、コンテンツ管理プログラム51は、記憶しているストレージ鍵253でコンテンツ鍵252を復号する。コンテンツ管理プログラム51は、コンテンツ鍵で暗号化されているコンテンツ251、および平文のコンテンツ鍵をグループゲートウェイプログラム61に供給する。

【0165】ステップS33において、グループゲートウェイプログラム61は、予め記憶しているグループ鍵271で、コンテンツ鍵を暗号化してコンテンツ鍵272を生成する。

【0166】ステップS34において、グループゲートウェイプログラム61は、コンテンツ鍵で暗号化されているコンテンツ251、およびグループ鍵271で暗号化されているコンテンツ鍵272を出力して、処理は終了する。

【0167】このように、パーソナルコンピュータ1は、コンテンツ鍵で暗号化されているコンテンツ251、およびグループ鍵271で暗号化されているコンテンツ鍵272を出力することができる。

【0168】次に、パーソナルコンピュータ1のコンテンツ251をインポートする処理について図15のフローチャートを参照して説明する。ステップS1201において、グループゲートウェイプログラム61は、ネットワーク2を介して、または光磁気ディスク93などの記録媒体を介して、コンテンツ鍵で暗号化されているコンテンツ251、およびグループ鍵271で暗号化されているコンテンツ鍵272を取得する。ステップS1202において、グループゲートウェイプログラム61は、キーボード78などの操作に対応して、グループのIDおよびパスワードを取得する。

【0169】ステップS1203において、グループゲートウェイプログラム61は、記憶しているグループのIDおよびパスワードを基に、ステップS1202の処理で取得されたグループのIDおよびパスワードが正しいかどうかを判定し、グループのIDおよびパスワードが正しいと判定された場合、ステップS1204に進み、ネットワーク2を介して、グループのIDおよびパスワードを承認サーバ3に送信する。

【0170】ステップS2201において、承認サーバ3は、パーソナルコンピュータ1から送信されたグループのIDおよびパスワードを受信する。ステップS2202において、承認サーバ3は、記録しているグループのIDおよびパスワードを基に、ステップS2201の処理で受信したグループのIDおよびパスワードが正しいかどうかを判定し、グループのIDおよびパスワードが正しいと判定された場合、ステップS2203に進み、ネットワーク2を介して、パーソナルコンピュータ1を承認する旨のデータを送信する。

【0171】ステップS1205において、グループゲートウェイプログラム61は、承認サーバ3から送信された承認する旨のデータを受信する。ステップS1206において、グループゲートウェイプログラム61は、グループ鍵271でコンテンツ鍵272を復号する。グループゲートウェイプログラム61は、復号したコンテンツ鍵をコンテンツ管理プログラム51に供給する。ステップS1207において、コンテンツ管理プログラム51は、コンテンツ鍵をストレージ鍵253で暗号化する。ステップS1208において、コンテンツ管理プログラム51は、コンテンツ鍵で暗号化されているコンテンツ251、およびストレージ鍵253で暗号化されているコンテンツ鍵252をコンテンツデータベース53に記録して、インポートの処理は終了する。

【0172】ステップS1203において、グループのIDおよびパスワードが正しくないと判定された場合、コンテンツ251のインポートを許可することはできないので、コンテンツ251をコンテンツデータベース53に記録せずに、処理は終了する。

【0173】ステップS2202において、グループのIDおよびパスワードが正しくないと判定された場合、

パーソナルコンピュータ1を承認することはできないので、コンテンツ251をコンテンツデータベース53に記録せずに、処理は終了する。

【0174】このように、パーソナルコンピュータ1は、正しいIDおよびパスワードが入力され、承認サーバ3に承認されたとき、コンテンツ251をインポートする。

【0175】図16は、グループのIDおよびパスワードの管理方法の他の例を説明する図である。

【0176】登録の処理において、パーソナルコンピュータ1は、承認サーバ3に、クレジットカードの番号などの課金情報を送信する。承認サーバ3は、ID管理サーバ8にクレジットカードの番号を送信し、ID管理サーバ8からグループのIDおよびパスワードを取得する。

【0177】ID管理サーバ8は、承認サーバ3からそのクレジットカードの番号を初めて受信したとき、クレジットカードの番号を含むグループのIDおよびパスワードを生成して、クレジットカードの番号に対応させてグループのIDおよびパスワードを記録すると共に、グループのIDおよびパスワードを承認サーバ3に送信する。ID管理サーバ8は、承認サーバ3から受信したクレジットカードの番号が既に記録されているとき（例えば、EMDサーバ4により既に登録されているとき）、クレジットカードの番号に対応して登録されているIDおよびパスワードをグループのIDおよびパスワードとして承認サーバ3に送信する。

【0178】承認サーバ3は、グループのIDおよびパスワードをパーソナルコンピュータ1に送信する。

【0179】ID管理サーバ8は、EMDサーバ4からそのクレジットカードの番号を初めて受信したとき、クレジットカードの番号を含むIDおよびパスワードを生成して、クレジットカードの番号に対応させてIDおよびパスワードを記録すると共に、IDおよびパスワードをEMDサーバ4に送信する。ID管理サーバ8は、EMDサーバ4から受信したクレジットカードの番号が記録されているとき（例えば、承認サーバ3により既に登録されているとき）、クレジットカードの番号に対応して登録されているIDおよびパスワードをEMDサーバ4に送信する。

【0180】EMDサーバ4は、IDおよびパスワードをパーソナルコンピュータ1に送信する。

【0181】このようにすることで、承認サーバ3に登録してからEMDサーバ4に登録しても、EMDサーバ4に登録してから承認サーバ3に登録しても、いずれの場合も、グループのIDおよびパスワードは、EMDサーバ4に登録したIDおよびパスワードと同一となる。

【0182】従って、グループのID、およびパスワードを知っている使用者は、グループのIDおよびパスワードを入力するだけで、EMDサーバ4からコンテンツ

を購入することができる。コンテンツを販売したEMDサーバ4は、入力されたグループのIDおよびパスワードを基に、ID管理サーバ8からクレジットカードの番号を読み出して、コンテンツの購入に対する課金の処理を実行する。

【0183】このようにすることで、グループのIDおよびパスワードを他の者に知られると使用者が不測の不利益を被る可能性が高くなるので、グループに属するパーソナルコンピュータ1を使用する使用者は、グループのIDおよびパスワードを他の者に知らせることがない。従って、パーソナルコンピュータ1から出力されるコンテンツは、不正に利用されることなく、複数の機器で利用することが可能になる。

【0184】次に、ID管理サーバ8がIDおよびパスワードを生成するときの、登録の処理を図17のフローチャートを参照して説明する。

【0185】ステップS1301において、グループゲートウェイプログラム61は、キーボード78の操作などにより入力されたクレジットカードの番号を取得する。ステップS1302において、グループゲートウェイプログラム61は、コンテンツ管理プログラム51からIDを取得して、コンテンツ管理プログラム51のIDおよびクレジットカードの番号を、ネットワーク2を介して、承認サーバ3に送信する。

【0186】ステップS2301において、承認サーバ3は、パーソナルコンピュータ1から送信されたコンテンツ管理プログラム51のIDおよびクレジットカードの番号を受信する。ステップS2302において、承認サーバ3は、クレジットカードの番号などを基に、パーソナルコンピュータ1がグループの1台目のパーソナルコンピュータであるか否かを判定し、パーソナルコンピュータ1がグループの1台目のパーソナルコンピュータであると判定された場合、ステップS2303に進み、グループ鍵271を生成する。ステップS2304において、承認サーバ3は、ネットワーク2を介して、クレジットカードの番号をID管理サーバ8に送信する。

【0187】ステップS3301において、ID管理サーバ8は、クレジットカードの番号を受信する。ステップS3302において、ID管理サーバ8は、IDおよびパスワードの生成の処理を実行する。ステップS3303において、ID管理サーバ8は、ネットワーク2を介して、IDおよびパスワードを承認サーバ3に送信する。

【0188】ステップS2305において、承認サーバ3は、IDおよびパスワードを受信する。ステップS2306において、承認サーバ3は、使用者に対応するアカウントを生成し、手続きは、ステップS2307に進む。

【0189】ステップS2302において、パーソナルコンピュータ1がグループの1台目のパーソナルコンピ

ュータでない、すなわち、2台目以降のパーソナルコンピュータ1であると判定された場合、グループ鍵271およびアカウントの生成の処理は不要なので、ステップS2303乃至ステップS2306の処理はスキップされ、手続きは、ステップS2307に進む。

【0190】ステップS2307乃至ステップS1305の処理のそれぞれは、図12に示すステップS2106乃至ステップS1105の処理のそれぞれと同様であるので、その説明は省略する。

【0191】次に、図17のステップS3302の処理に対応する、ID管理サーバ8によるIDおよびパスワードの生成の処理の例を図18のフローチャートを参照して説明する。

【0192】ステップS51において、ID管理サーバ8は、受信の処理により取得したクレジットカードの番号が登録されているか否かを判定し、クレジットカードの番号が登録されていないと判定された場合、ステップS52に進み、IDおよびパスワードを生成する。ステップS52の処理において、生成されるグループのIDおよびパスワードのいずれかは、クレジットカードの番号と同一である。

【0193】ステップS53において、ID管理サーバ8は、クレジットカードの番号と、IDおよびパスワードを対応させて記録して、処理は終了する。

【0194】ステップS51において、クレジットカードの番号が登録されていると判定された場合、ステップS54に進み、ID管理サーバ8は、クレジットカードの番号に対応して記録されている、IDおよびパスワードを読み出して、処理は終了する。

【0195】次に、パーソナルコンピュータ1およびEMDサーバ4による登録の処理を図19のフローチャートを参照して説明する。ステップS1401において、パーソナルコンピュータ1は、キーボード78などの操作に対応して、クレジットカードの番号を取得する。ステップS1402において、パーソナルコンピュータ1は、ネットワーク2を介して、EMDサーバ4に、クレジットカードの番号を送信する。

【0196】ステップS2401において、EMDサーバ4は、パーソナルコンピュータ1が送信したクレジットカードの番号を受信する。ステップS2402において、EMDサーバ4は、ネットワーク2を介して、ID管理サーバ8にクレジットカードの番号を送信する。

【0197】ステップS3401において、ID管理サーバ8は、EMDサーバ4が送信したクレジットカードの番号を受信する。ステップS3402において、ID管理サーバ8は、IDおよびパスワードを生成する。ステップS3402の処理の詳細は、図18のフローチャートを参照して説明した処理と同様なので、その説明は省略する。

【0198】ステップS3403において、ID管理サ

ーバ8は、ネットワーク2を介して、IDおよびパスワードをEMDサーバ4に送信する。

【0199】ステップS2403において、EMDサーバ4は、IDおよびパスワードを受信する。ステップS2404において、EMDサーバ4は、アカウントを生成する。ステップS2405において、EMDサーバ4は、ネットワーク2を介して、IDおよびパスワードをパーソナルコンピュータ1に送信する。

【0200】ステップS1403において、パーソナルコンピュータ1は、IDおよびパスワードを受信する。ステップS1404において、パーソナルコンピュータ1は、受信したIDおよびパスワードを表示して、処理は終了する。

【0201】このように、承認サーバ3が発行するグループのIDおよびパスワードは、EMDサーバ4が発行するIDおよびパスワードと共通とすることができる。

【0202】次に、EMDサーバ4からコンテンツを購入したときに実行する決済の処理を図20のフローチャートを参照して説明する。ステップS1501において、パーソナルコンピュータ1は、キーボード78などの操作に対応して、グループのIDおよびパスワードまたはEMDサーバ4に登録して取得したIDおよびパスワードを取得する。ステップS1502において、パーソナルコンピュータ1は、ネットワーク2を介して、IDおよびパスワードと共に、決済の要求をEMDサーバ4に送信する。

【0203】ステップS2501において、EMDサーバ4は、パーソナルコンピュータ1から送信されたID、パスワード、および決済の要求を受信する。ステップS2502において、EMDサーバ4は、ネットワーク2を介して、IDおよびパスワードをID管理サーバ8に送信する。

【0204】ステップS3501において、ID管理サーバ8は、EMDサーバ4から送信されたIDおよびパスワードを受信する。ステップS3502において、ID管理サーバ8は、IDおよびパスワードに対応するクレジットカード番号を読み出す。ステップS3503において、ID管理サーバ8は、ネットワーク2を介して、クレジットカード番号をEMDサーバ4に送信する。

【0205】ステップS2503において、EMDサーバ4は、ID管理サーバ8から送信したクレジットカード番号を受信する。ステップS2504において、EMDサーバ4は、受信したクレジットカード番号を基に、課金の処理を実行して、処理は終了する。

【0206】このように、EMDサーバ4は、グループのIDおよびパスワード、またはEMDサーバ4に登録して取得したIDおよびパスワードのいずれかで、課金の処理を実行することができる。

【0207】次に、パーソナルコンピュータ1がコンテ

ンツをインポートする他の処理について図21を参照して説明する。

【0208】この例において、パーソナルコンピュータ1のグループゲートウェイプログラム61は、承認サーバ3に登録したとき、グループ鍵を取得せず、グループのIDおよびパスワードのみを取得する。

【0209】グループゲートウェイプログラム61は、コンテンツ251のインポートが要求され、使用者によりグループのIDおよびパスワードが入力された場合、ネットワーク2を介して、グループのIDおよびパスワードを解読認証サーバ331に送信する。解読認証サーバ331は、パーソナルコンピュータ1から送信されたグループのIDおよびパスワードを受信すると、グループのIDおよびパスワードを更に承認サーバ3に送信する。

【0210】承認サーバ3は、解読認証サーバ331から送信されたグループのIDおよびパスワードを受信すると、予め記録しているグループのIDおよびパスワードを基に、受信したグループのIDおよびパスワードが正しいか否かを判定し、その判定結果を解読認証サーバ331に送信する。

【0211】解読認証サーバ331は、グループのIDおよびパスワードが正しいと判定された場合、グループのIDおよびパスワードを基に、グループ鍵271を生成して、ネットワーク2を介して、グループ鍵271をパーソナルコンピュータ1に送信する。

【0212】一方、グループのIDおよびパスワードが正しくないと判定された場合、解読認証サーバ331は、グループ鍵271を生成しないで処理を終了する。

【0213】このように、例えば、何らかの理由で無効になったグループのIDおよびパスワードを基に、グループ鍵271の生成が要求されたとき、解読認証サーバ331は、グループ鍵271を生成しない。

【0214】また、解読認証サーバ331は、コンテンツが復号される度に、グループ鍵271を生成するので、コンテンツの利用状況を知ることができる。

【0215】以上のように、グループゲートウェイプログラム61は、グループ鍵271を保持せず、また、グループ鍵271を生成する手続きを有していないので、パーソナルコンピュータ1は、より強固にコンテンツ251の不正なインポートを防止することができる。

【0216】図22のフローチャートを参照して、解読認証サーバ331が実行するグループ鍵271の送信の処理を説明する。ステップS71において、解読認証サーバ331は、ネットワーク2を介して、パーソナルコンピュータ1から送信されたグループのIDおよびパスワードを受信する。ステップS72において、解読認証サーバ331は、グループのIDおよびパスワードを承認サーバ3に送信して、承認サーバ3にグループのIDおよびパスワードが正当であるかを問い合わせ、承認サ

ーバ3から、グループのIDおよびパスワードが正当であるか否かを示すデータを受信する。

【0217】ステップS73において、解読認証サーバ331は、承認サーバ3から受信したデータを基に、グループのIDおよびパスワードが正当であるか否かを判定し、グループのIDおよびパスワードが正当であると判定された場合、ステップS74に進み、グループのIDおよびパスワードを基に、グループ鍵271を生成する。ステップS75において、解読認証サーバ331は、ネットワーク2を介して、生成したグループ鍵271をパーソナルコンピュータ1に送信して、処理は終了する。

【0218】ステップS73において、グループのIDおよびパスワードが正当でないと判定された場合、インポートを許可することができないので、解読認証サーバ331は、グループ鍵271をパーソナルコンピュータ1に送信しないで、処理は終了する。

【0219】このように、解読認証サーバ331は、パーソナルコンピュータ1からグループのIDおよびパスワードを受信して、グループのIDおよびパスワードが正当であるとき、グループ鍵271を生成してパーソナルコンピュータ1に送信し、グループのIDおよびパスワードが正当でないとき、グループ鍵271を生成しない。従って、パーソナルコンピュータ1は、正当なグループのIDおよびパスワードが入力されたときに限り、コンテンツ251をインポートすることができる。

【0220】次に、ロッカーサーバ11の動作について説明する。

【0221】図23は、ロッカーサーバ11への登録の処理を説明する図である。ロッカーサーバ11は、コンテンツデータベース401と接続され、ログデータベース402と接続されている。

【0222】ロッカーサーバ11は、ネットワーク2を介して、パーソナルコンピュータ1から供給されたコンテンツデータベース401に記録させる。

【0223】コンテンツデータベース401は、登録されているパーソナルコンピュータ1からロッカーサーバ11が受信したコンテンツを記録し、ロッカーサーバ11からの要求に対応して、記録されているコンテンツをロッカーサーバ11に供給する。

【0224】ロッカーサーバ11は、ネットワーク2を介して、コンテンツデータベース401から供給されたコンテンツをパーソナルコンピュータ1に送信する。

【0225】ログデータベース402は、ロッカーサーバ11へのパーソナルコンピュータ1の登録の処理、コンテンツの記録の処理、またはコンテンツの読み出しの処理に対応するログを記録する。

【0226】パーソナルコンピュータ1は、ロッカーサーバ11への登録を要求するとき、クレジットカードの番号をロッカーサーバ11に送信する。

【0227】ロッカーサーバ11は、IDを生成して、生成したIDをログデータベース402に記録させると共に、生成したIDをパーソナルコンピュータ1に送信する。ロッカーサーバ11が生成するIDは、例えば、パーソナルコンピュータ1の使用者のクレジットカードの番号と同一である。

【0228】ロッカーサーバ11は、パーソナルコンピュータ1を登録した旨を示すログをパーソナルコンピュータ1に送信すると共に、登録に対応する課金の処理を実行して、その結果をパーソナルコンピュータ1に送信する。

【0229】図24は、ロッカーサーバ11が記録しているコンテンツのリストの例を説明する図である。ロッカーサーバ11は、登録している使用者のIDに対応させて、コンテンツの名称を記録する。

【0230】例えば、ロッカーサーバ11は、“aaaaa”である使用者のIDに対応させて、“イイイイイ”であるコンテンツの名称を記録し、“bbbbbb”である使用者のIDに対応させて、“ロロロロロ”であるコンテンツの名称を記録し、“cccccc”である使用者のIDに対応させて、“ハハハハハ”であるコンテンツの名称を記録する。

【0231】図25は、ロッカーサーバ11によるコンテンツの共用を説明する図である。ロッカーサーバ11は、パーソナルコンピュータ1-1から供給されたコンテンツをコンテンツデータベース401に記録させる。ロッカーサーバ11は、コンテンツのリストに、パーソナルコンピュータ1-1の使用者のIDに対応させてコンテンツの名称を記録すると共に、パーソナルコンピュータ1-1から供給されたコンテンツをコンテンツデータベース401に記録させた旨のログをログデータベース402に記録させる。

【0232】パーソナルコンピュータ1-1と同一のIDを基に、パーソナルコンピュータ1-2からコンテンツの送信が要求されたとき、ロッカーサーバ11は、コンテンツのリストを基に、使用者のIDが正しいか否かを判定し、使用者のIDが正しいと判定された場合、コンテンツデータベース401にコンテンツの供給を要求する。ロッカーサーバ11は、コンテンツデータベース401から供給されたコンテンツをパーソナルコンピュータ1-2に送信する。ロッカーサーバ11は、パーソナルコンピュータ1-2にコンテンツを供給した旨を示すログをログデータベース402に記録させる。

【0233】図26に示すように、パーソナルコンピュータ1-1は、EMDサーバ4から購入したコンテンツをロッカーサーバ11に送信し、コンテンツデータベース401に記録させることもできる。この場合も、パーソナルコンピュータ1-1と同一のIDを基に、パーソナルコンピュータ1-2からコンテンツの送信が要求されたとき、ロッカーサーバ11は、パーソナルコンピ

ータ1-1と同一のIDを基に、コンテンツデータベース401にコンテンツの供給を要求し、コンテンツデータベース401から供給されたコンテンツをパーソナルコンピュータ1-2に送信する。

【0234】図27に示すように、ロッカーサーバ11は、パーソナルコンピュータ1を登録した旨を示すログをパーソナルコンピュータ1に送信すると共に、登録に対応して月極の課金の処理を実行して、その結果をパーソナルコンピュータ1に送信するようにしてもよい。

【0235】次に、図28のフローチャートを参照して、パーソナルコンピュータ1およびロッカーサーバ11による登録の処理を説明する。

【0236】ステップS1601において、パーソナルコンピュータ1は、キーボード78の操作などにより入力されたクレジットカードの番号を取得する。ステップS1602において、パーソナルコンピュータ1は、クレジットカードの番号を、ネットワーク2を介して、ロッカーサーバ11に送信する。

【0237】ステップS2601において、ロッカーサーバ11は、パーソナルコンピュータ1から送信されたクレジットカードの番号を受信する。ステップS2602において、ロッカーサーバ11は、受信したクレジットカードの番号を基に、初めて登録されたか否かを判定し、初めて登録されたと判定された場合、ステップS2603に進み、使用者のIDを生成する。ステップS2604において、ロッカーサーバ11は、生成した使用者のIDを記録して、ステップS2605に進む。

【0238】ステップS2602において、初めて登録されたのではないと判定された場合、IDの生成の処理は必要ないので、ステップS2603の処理およびステップS2604の処理はスキップされ、手続きは、ステップS2605に進む。

【0239】ステップS2605において、ロッカーサーバ11は、使用者のIDを登録した旨のログをログデータベース402に記録させる。ステップS2606において、ロッカーサーバ11は、ネットワーク2を介して、使用者のID、およびログをパーソナルコンピュータ1に送信する。

【0240】ステップS1603において、パーソナルコンピュータ1は、ロッカーサーバ11から送信された使用者のID、およびログを受信する。ステップS1604において、パーソナルコンピュータ1は、使用者のID、およびログを記録する。ステップS2607において、ロッカーサーバ11は、受信したクレジットカードの番号を基に、初めて登録されたか否かを判定し、初めて登録されたと判定された場合、ステップS2608に進み、受信したクレジットカードの番号を基に、課金の処理を実行して、処理は終了する。

【0241】ステップS2607において、初めて登録されたのではないと判定された場合、課金の処理は不要

なので、ステップS2608の処理はスキップされ、処理は終了する。

【0242】このように、パーソナルコンピュータ1は、ロッカーサーバ11に、クレジットカードの番号を送信することにより、使用者のIDを取得することができる。一方、ロッカーサーバ11は、パーソナルコンピュータ1の登録の際に、クレジットカードの番号を取得し、生成した使用者のIDと共に、取得したクレジットカードの番号を記録することができる。

【0243】次に、図29のフローチャートを参照して、ロッカーサーバ11へのコンテンツの記録の処理を説明する。ステップS1701において、パーソナルコンピュータ1は、ネットワーク2を介して、使用者のIDと共にコンテンツをロッカーサーバ11に送信する。

【0244】ステップS2701において、ロッカーサーバ11は、パーソナルコンピュータ1から送信された使用者のIDおよびコンテンツを受信する。ステップS2702において、ロッカーサーバ11は、リストに記録している使用者のIDを基に、受信した使用者のIDが登録されているか否かを判定し、受信した使用者のIDが登録されていると判定された場合、ステップS2703に進み、受信したコンテンツをコンテンツデータベース401に記録させる。

【0245】ステップS2704において、ロッカーサーバ11は、コンテンツを記録した旨のログをログデータベース402に記録させる。ステップS2705において、ロッカーサーバ11は、ネットワーク2を介して、コンテンツを記録した旨のログをパーソナルコンピュータ1に送信する。

【0246】ステップS1702において、パーソナルコンピュータ1は、ロッカーサーバ11から送信された、コンテンツを記録した旨のログを受信する。ステップS1703において、パーソナルコンピュータ1は、受信したログを記録する。ステップS1704において、パーソナルコンピュータ1は、受信したログをディスプレイ80に表示させ、処理は終了する。

【0247】ステップS2702において、受信した使用者のIDが登録されていないと判定された場合、不正なコンテンツの記録の要求なので、コンテンツを記録しないで処理は終了する。

【0248】このように、ロッカーサーバ11は、正しいIDと共にコンテンツを受信したとき、コンテンツをコンテンツデータベース401に記録させ、不正なIDと共にコンテンツを受信したとき、受信したコンテンツを破棄する。

【0249】次に、図30のフローチャートを参照して、ロッカーサーバ11からのコンテンツの読み出しの処理を説明する。ステップS1801において、パーソナルコンピュータ1は、ネットワーク2を介して、使用者のIDと共にコンテンツの要求をロッカーサーバ11

に送信する。

【0250】ステップS2801において、ロッカーサーバ11は、パーソナルコンピュータ1から送信された使用者のIDおよびコンテンツの要求を受信する。ステップS2802において、ロッカーサーバ11は、記録している使用者のIDを基に、受信した使用者のIDが登録されているか否かを判定し、受信した使用者のIDが登録されていると判定された場合、ステップS2803に進み、コンテンツデータベース401からコンテンツを読み出す。

【0251】ステップS2804において、ロッカーサーバ11は、コンテンツの読み出しに対応するログをログデータベース402に記録させる。ステップS2805において、ロッカーサーバ11は、ネットワーク2を介して、読み出したコンテンツ、およびコンテンツの読み出した旨のログをパーソナルコンピュータ1に送信する。

【0252】ステップS1802において、パーソナルコンピュータ1は、ロッカーサーバ11から送信されたコンテンツおよびログを受信する。ステップS1803において、パーソナルコンピュータ1は、受信したコンテンツおよびログを記録する。ステップS1804において、パーソナルコンピュータ1は、受信したログをディスプレイ80に表示させ、処理は終了する。

【0253】ステップS2802において、受信した使用者のIDが登録されていないと判定された場合、不正なコンテンツの要求なので、コンテンツを送信しないで処理は終了する。

【0254】このように、ロッカーサーバ11は、登録されている使用者のIDと共にコンテンツの要求を受信したとき、コンテンツデータベース401からコンテンツを読み出して、読み出したコンテンツを送信し、使用者のIDが登録されていないとき、コンテンツ送信しない。

【0255】次に、本発明に係る音楽データ管理システムの第2の実施の形態について説明する。

【0256】図31は、本発明に係る音楽データ管理システムの第2の実施の形態を示す図である。公衆回線網503には、通信サービスの提供エリアを所望の広さに分割したセルにそれぞれ配置されている、固定無線局である基地局502-1乃至502-4を介して、PDA501-1若しくは501-2、またはカメラ付きデジタル携帯電話機16-1若しくは16-2が接続されている。

【0257】基地局502-1乃至502-4は、移動無線局であるPDA501-1および501-2、並びにカメラ付きデジタル携帯電話機16-1および16-2を、例えば、W-CDMA(Wideband-Code Division Multiple Access)と呼ばれる符号分割多元接続により無線接続し、移動無線局であるPDA501-1および501-

2、並びにカメラ付きデジタル携帯電話機16-1および16-2と、2GHzの周波数帯域を利用して最大2Mbpsのデータ転送速度で大容量データを高速にデータ通信できる。

【0258】PDA501-1および501-2、並びにカメラ付きデジタル携帯電話機16-1および16-2は、基地局502-1乃至502-4とW-CDMA方式により大容量データを高速にデータ通信できるので、音声通話に限らず、電子メールの送受信、簡易ホームページの閲覧、画像などのコンテンツの送受信等の多種に及ぶデータ通信を実行し得る。

【0259】PDA501-1若しくは501-2、またはカメラ付きデジタル携帯電話機16-1若しくは16-2は、ブラウザプログラム、コンテンツ管理プログラム51、またはグループゲートウェイプログラム61などを実行し、コンテンツの管理またはコンテンツの入出力に使用される。

【0260】また、基地局502-1乃至502-4は、有線回線を介して、公衆回線網503に接続されている。公衆回線網503には、インターネット、ネットワーク2、図示せぬ加入者有線端末装置、コンピュータネットワーク、および企業内ネットワーク等が接続されている。

【0261】インターネットサービスプロバイダのアクセスサーバ504は、公衆回線網503に接続されており、更に、インターネットサービスプロバイダが保有するコンテンツサーバ505に接続されている。

【0262】コンテンツサーバ505は、加入者有線端末装置、PDA501-1若しくは501-2、またはカメラ付きデジタル携帯電話機16-1若しくは16-2からの要求に対応して、例えば、簡易ホームページ等のコンテンツを、コンパクトHTML (HyperText Markup Language) 方式のファイルとして提供する。

【0263】ネットワーク2には、多数のWWW (World Wide Web) サーバ506-1乃至506-Nが接続されている。WWWサーバ506-1乃至506-Nは、TCP (Transmission Control Protocol) / IP (Internet Protocol) のプロトコルに従って、加入者有線端末装置、PDA501-1および1-2、並びにカメラ付きデジタル携帯電話機16-1および16-2からアクセスされる。

【0264】WWWサーバ506-1乃至506-Nは、承認サーバ3、EMDサーバ4、ID管理サーバ8、またはロッカーサーバ11と同様の処理を実行し、ネットワーク2を介して、PDA501-1若しくは501-2、またはカメラ付きデジタル携帯電話機16-1若しくは16-2に、コンテンツなどを提供すると共に、コンテンツを記録し、若しくは送信し、またはIDなどを管理する。

【0265】因みに、PDA501-1および501-2、並びにカメラ付きデジタル携帯電話機16-1およ

び16-2は、基地局502-1乃至502-4までを2Mbpsの簡易トランスポートプロトコルで通信し、基地局502-1乃至502-4から、ネットワーク2、およびWWWサーバ506-1乃至506-NまでをTCP/IPで通信する。

【0266】なお、管理制御装置507は、公衆回線網503を介して、加入者有線端末装置、PDA501-1および1-2、並びにカメラ付きデジタル携帯電話機16-1および16-2に接続され、加入者有線端末装置、PDA501-1および501-2、並びにカメラ付きデジタル携帯電話機16-1および16-2に対する認証処理または課金処理などを実行する。

【0267】カメラ付きデジタル携帯電話機16-1および16-2は、公衆回線網503およびネットワーク2を介して、上述した、パーソナルコンピュータ1と同様の処理でコンテンツを利用する。

【0268】以下、カメラ付きデジタル携帯電話機16-1および16-2を個々に区別する必要がないとき、単に、カメラ付きデジタル携帯電話機16と称する。

【0269】次に本発明を適用したカメラ付デジタル携帯電話機16の外観構成について説明する。図32に示すようにカメラ付デジタル携帯電話機16は、表示部531および本体532で構成され、中央のヒンジ部533により折り畳み可能に形成されている。

【0270】表示部531は、上端左部に引出しまたは収納可能な送受信用のアンテナ534を有する。カメラ付デジタル携帯電話機16は、アンテナ534を介して、固定無線局である基地局502-1乃至502-4のいずれかとの間で電波を送受信する。

【0271】また、表示部531は、上端中央部にほぼ180度の角度範囲で回動自在なカメラ部535を有する。カメラ付デジタル携帯電話機16は、カメラ部535のCCDカメラ536によって所望の撮像対象を撮像する。

【0272】カメラ部535が使用者によってほぼ180度回動されて位置決めされた場合、図33に示すように、表示部531は、カメラ部535の背面側中央に設けられたスピーカ537が正面側に位置する状態となる。これにより、カメラ付デジタル携帯電話機16は、通常の音声通話状態に切り換わる。

【0273】さらに、表示部531の正面に液晶ディスプレイ538が設けられている。液晶ディスプレイ538は、電波の受信状態、電池残量、電話帳として登録されている相手先名や電話番号および発信履歴等の他、電子メールの内容、簡易ホームページ、カメラ部535のCCDカメラ536で撮像した画像などを表示する。

【0274】一方、本体532には、その表面に「0」乃至「9」の数字キー、発呼キー、リダイヤルキー、終話及び電源キー、クリアキー及びメールキー等の操作キー539が設けられている。操作キー539の操作に対

応した各種指示が、カメラ付デジタル携帯電話機16に  
入力される。

【0275】また、本体532の操作キー539の下部  
にメモボタン540およびマイクロフォン541が設け  
られている。カメラ付デジタル携帯電話機16は、メモ  
ボタン540が操作されたとき、通話中の相手の音声  
を録音する。カメラ付デジタル携帯電話機16は、マイク  
ロフォン541によって通話時の使用者の音声を集音す  
る。

【0276】さらに、本体532の操作キー539の上  
部に回動自在なジョグダイヤル542が、本体532の  
表面から僅かに突出した状態で設けられている。カメラ  
付デジタル携帯電話機16は、ジョグダイヤル542に  
対する回動操作に応じて、液晶ディスプレイ538に表  
示されている電話帳リスト若しくは電子メールのスクロ  
ール動作、簡易ホームページのページ捲り動作、または  
画像の送り動作等の種々の動作を実行する。

【0277】例えば、本体532は、使用者によるジョ  
グダイヤル542の回動操作に応じて液晶ディスプレイ  
538に表示された電話帳リストの複数の電話番号の中  
から所望の電話番号を選択し、ジョグダイヤル542が  
本体532の内部方向に押圧されたとき、選択されてい  
る電話番号を確定して、確定した電話番号に対して自動  
的に発呼処理を行う。

【0278】なお、本体532は、背面側に図示しない  
バッテリーパックが装着されており、終話／電源キーがオ  
ン状態になると、バッテリーパックから各回路部に対して  
電力が供給されて動作可能な状態に起動する。

【0279】ところで、本体532の左側面上部に拔差  
自在なメモリカード13を装着するためのメモリカード  
スロット543が設けられている。カメラ付デジタル携  
帯電話機16は、メモボタン540が押下されると、通  
話中の相手の音声を装着されているメモリカード13に  
記録する。カメラ付デジタル携帯電話機16は、使用者  
の操作に応じて、電子メール、簡易ホームページ、CC  
Dカメラ536で撮像した画像、または音声などのコン  
テンツを装着されているメモリカード13に記録する。

【0280】メモリカード13は、例えば、メモリス  
ティック（商標）である。メモリスティックは、本願  
出願人であるソニー株式会社によって開発されたフラッ  
シュメモリカードの一種である。このメモリカード13  
は、縦21.5×横50×厚さ2.8[mm]の小型薄型形状のプラス  
チックケース内に電気的に書換えや消去が可能な不揮発  
性メモリであるEEPROM（Electrically Erasable and Pr  
ogrammable Read Only Memory）の一種であるフラッ  
シュメモリ素子を格納したものであり、10ピン端子を介  
して画像や音声、音楽等の各種データの書き込み及び読  
み出しが可能となっている。

【0281】またメモリスティックは、大容量化等  
による内蔵フラッシュメモリの仕様変更に対しても、使用

する機器で互換性を確保することができる独自のシリア  
ルプロトコルを採用し、最大書込速度1.5[MB/S]、最大  
読出速度2.45[MB/S]の高速性能を実現していると共に、  
誤消去防止スイッチを設けて高い信頼性を確保してい  
る。

【0282】従って、カメラ付デジタル携帯電話機16  
は、このようなメモリカード13を装着可能に構成され  
ているために、メモリカード13を介して、他の電子機  
器との間でデータの共有化を図ることができる。

10 【0283】図34に示すように、カメラ付デジタル携  
帯電話機16は、表示部531および本体532の各部  
を統括的に制御する主制御部551に対して、電源回路  
部552、操作入力制御部553、画像エンコーダ55  
4、カメラインターフェース部555、LCD（Liquid Cr  
ystal Display）制御部556、画像デコーダ557、  
多重分離部558、記憶再生部563、変復調回路部5  
59、および音声コーデック560がメインバス561  
を介して互いに接続されると共に、画像エンコーダ55  
4、画像デコーダ557、多重分離部558、変復調回  
20 路部559、および音声コーデック560が同期バス5  
62を介して互いに接続されて構成されている。

【0284】電源回路部552は、使用者の操作により  
終話／電源キーがオン状態にされると、バッテリーパッ  
クから各部に対して電力を供給することによりカメラ付デ  
ジタル携帯電話機16を動作可能な状態に起動する。

【0285】カメラ付デジタル携帯電話機16は、CP  
U、ROMおよびRAM等である主制御部551の制御  
に基づいて、音声通話モードにおいて、マイクロフォン  
541で集音した音声信号を音声コーデック560によ  
ってデジタル音声データに変換する。カメラ付デジタル  
30 携帯電話機16は、デジタル音声データを变復調回路部  
559でスペクトラム拡散処理し、送受信回路部564  
でデジタルアナログ変換処理および周波数変換処理を施  
した後にアンテナ534を介して送信する。

【0286】また、カメラ付デジタル携帯電話機16  
は、音声通話モードにおいて、アンテナ534で受信し  
た受信信号を増幅して周波数変換処理およびアナログデ  
ジタル変換処理を施し、変復調回路部559でスペク  
40 トラム逆拡散処理し、音声コーデック560によってアナ  
ログ音声信号に変換する。カメラ付デジタル携帯電話機  
16は、アナログ音声信号に対応する音声をスピーカ5  
37に出力させる。

【0287】さらに、カメラ付デジタル携帯電話機16  
は、データ通信モードにおいて、コンテンツを送信する  
場合、操作キー539およびジョグダイヤル542の操  
作によって入力に対応して指定されたコンテンツを主制  
御部551に送出する。

【0288】主制御部551は、コンテンツを変復調回  
路部559でスペクトラム拡散処理し、送受信回路部5  
50 64でデジタルアナログ変換処理及び周波数変換処理を



施した後にアンテナ534を介して基地局へ送信する。

【0289】これに対してカメラ付デジタル携帯電話機16は、データ通信モードにおいて、コンテンツを受信する場合、アンテナ534を介して基地局CS3から受信した受信信号を変復調回路部559でスペクトラム逆拡散処理して、元のコンテンツを復元した後、LCD制御部556を介して液晶ディスプレイ538にコンテンツに対応するデータを表示する。

【0290】LCD制御部556は、フレキシブルプリント配線板11と同様に、パネルID設定部を有するフレキシブルプリント配線板を介して、液晶ディスプレイ538に接続されている。

【0291】この後、カメラ付デジタル携帯電話機16は、使用者の操作に応じて受信したコンテンツを記憶再生部563を介してメモリカード13に記録することも可能である。

【0292】カメラ付デジタル携帯電話機16は、データ通信モードにおいて画像データを送信する場合、CCDカメラ536で撮像された画像データをカメラインターフェース部555を介して画像エンコーダ554に供給する。

【0293】因みにカメラ付デジタル携帯電話機16は、画像データを送信しない場合には、CCDカメラ536で撮像した画像データをカメラインターフェース部555およびLCD制御部556を介して液晶ディスプレイ538に直接表示することも可能である。

【0294】画像エンコーダ554は、CCDカメラ536から供給された画像データを、例えば、MPEG(Movig Picture Experts Group)2またはMPEG4等の所定の符号化方式によって圧縮符号化することにより符号化画像データに変換し、これを多重分離部558に送出する。

【0295】このとき同時にカメラ付デジタル携帯電話機16は、CCDカメラ536で撮像中にマイクロフォン541で集音した音声を音声コーデック560を介してデジタルの音声データとして多重分離部558に送出する。

【0296】多重分離部558は、画像エンコーダ554から供給された符号化画像データと音声コーデック560から供給された音声データとを所定の方式で多重化し、その結果得られる多重化データを変復調回路部559でスペクトラム拡散処理し、送受信回路部564でデジタルアナログ変換処理及び周波数変換処理を施した後にアンテナ534を介して送信する。

【0297】これに対してカメラ付デジタル携帯電話機16は、データ通信モードにおいて、例えば、簡易ホームページ等にリンクされた動画像ファイルのデータを受信する場合、アンテナ534を介して基地局から受信した受信信号を変復調回路部559でスペクトラム逆拡散処理し、その結果得られる多重化データを多重分離部5

58に送出する。

【0298】多重分離部558は、多重化データを符号化画像データと音声データとに分離し、同期バス562を介して、符号化画像データを画像デコーダ557に供給すると共に、音声データを音声コーデック560に供給する。

【0299】画像デコーダ557は、符号化画像データをMPEG2またはMPEG4等の所定の符号化方式に対応した復号方式でデコードすることにより再生動画像データを生成し、これをLCD制御部556を介して液晶ディスプレイ538に供給する。これにより、カメラ付デジタル携帯電話機16は、例えば、簡易ホームページにリンクされた動画像ファイルに含まれる動画データを表示する。

【0300】このとき同時に音声コーデック560は、音声データをアナログ音声信号に変換した後、これをスピーカ537に供給する。これにより、カメラ付デジタル携帯電話機16は、例えば、簡易ホームページにリンクされた動画像ファイルに含まれる音声データを再生する。

【0301】なお、パーソナルコンピュータ1またはカメラ付きデジタル携帯電話機16は、クレジットカードの番号を送信し、承認サーバ3、ID管理サーバ8、またはロッカーサーバ11は、クレジットカードの番号を記録すると説明したが、クレジットカードの番号に限らず、銀行口座の番号またはインターネット接続サービスプロバイダの登録番号など課金の処理が可能な情報であればよい。

【0302】上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、プログラム格納媒体からインストールされる。

【0303】コンピュータにインストールされ、コンピュータによって実行可能な状態とされるプログラムを格納するプログラム格納媒体は、図3または図4に示すように、磁気ディスク91または131(フロッピーディスクを含む)、光ディスク92または132(CD-ROM(Compact Disc-Read Only Memory)、DVD(Digital Versatile Disc)を含む)、光磁気ディスク93または133(MD(Mini-Disc)を含む)、若しくは半導体メモリ94または134などよりなるパッケージメディア、または、プログラムが一時的若しくは永続的に格納されるROM72または102や、HDD81または111などにより構成される。プログラム格納媒体へのプログラムの格納は、必要に応じてルータ、モデムなどのインタフェ

ースを介して、ローカルエリアネットワーク、インターネット、デジタル衛星放送といった、有線または無線の通信媒体を利用して行われる。

【0304】なお、本明細書において、プログラム格納媒体に格納されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【0305】また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【0306】

【発明の効果】請求項1に記載の情報処理装置、請求項4に記載の情報処理方法、および請求項5に記載のプログラム格納媒体によれば、他の情報処理装置から送信された識別データが受信され、識別データを受信した場合、他の情報処理装置が属するグループにおいて共用されるグループ鍵が生成され、グループ鍵が、識別データに対応して記録され、グループ鍵が、他の情報処理装置へ送信されるようにしたので、正当な権利を有さない第三者の利用を防止しつつ、所望のコンテンツをグループに属する所望の情報処理装置で利用することができるようになる。

【0307】請求項6に記載の情報処理装置、請求項8に記載の情報処理方法、および請求項9に記載のプログラム格納媒体によれば、グループを特定するIDが記憶され、他の情報処理装置からグループを特定するIDが受信され、記憶されているIDと、受信されたIDとが比較され、比較結果に基づいて、他の情報処理装置に対して、その情報のコピー動作を承認するデータが出力されるようにしたので、正当な権利を有さない第三者の利用を防止しつつ、所望のコンテンツをグループに属する所望の情報処理装置で利用することができるようになる。

【0308】請求項10に記載の情報処理装置、請求項14に記載の情報処理方法、および請求項15に記載のプログラム格納媒体によれば、第1の他の情報処理装置に対して、識別データが送信され、第1の他の情報処理装置から、グループにおいて共用されるグループ鍵が受信され、受信されたグループ鍵が記憶され、コンテンツを出力する場合、コンテンツを暗号化しているコンテンツ鍵がグループ鍵で暗号化されるようにしたので、正当な権利を有さない第三者の利用を防止しつつ、所望のコンテンツをグループに属する所望の情報処理装置で利用することができるようになる。

【図面の簡単な説明】

【図1】従来のコンテンツを暗号化して記録し、復号して利用するプログラムを説明する図である。

【図2】本発明に係る音楽データ管理システムの一実施の形態を示す図である。

【図3】パーソナルコンピュータ1-1の構成を説明する図である。

【図4】承認サーバ3の構成を説明する図である。

【図5】パーソナルコンピュータ1-1の機能の構成を説明するブロック図である。

【図6】パーソナルコンピュータ1が記録しているコンテンツを説明する図である。

【図7】パーソナルコンピュータ1が出力するコンテンツを説明する図である。

10 【図8】コンテンツ251をインポートするパーソナルコンピュータ1-2の動作を説明する図である。

【図9】コンテンツのインポートのときの承認サーバ3の承認を説明する図である。

【図10】1つのグループに属するパーソナルコンピュータ1-1乃至1-3を承認サーバ3に登録する処理を説明する図である。

【図11】コンテンツをインポートするときの処理を説明する図である。

20 【図12】登録の処理を説明するフローチャートである。

【図13】グループのIDおよびパスワードの生成の処理の例を説明するフローチャートである。

【図14】コンテンツの出力の処理を説明するフローチャートである。

【図15】コンテンツをインポートする処理を説明するフローチャートである。

【図16】グループのIDおよびパスワードの管理方法の他の例を説明する図である。

30 【図17】登録の処理を説明するフローチャートである。

【図18】ID管理サーバ8によるIDおよびパスワードの生成の処理を説明するフローチャートである。

【図19】パーソナルコンピュータ1およびEMDサーバ4による登録の処理を説明するフローチャートである。

【図20】決済の処理を説明するフローチャートである。

【図21】コンテンツをインポートする他の処理を説明する図である。

40 【図22】グループ鍵271の送信の処理を説明するフローチャートである。

【図23】ロッカーサーバ11への登録の処理を説明する図である。

【図24】ロッカーサーバ11が記録しているコンテンツのリストの例を説明する図である。

【図25】ロッカーサーバ11によるコンテンツの共用を説明する図である。

【図26】ロッカーサーバ11によるコンテンツの共用を説明する図である。

50 【図27】ロッカーサーバ11による課金の処理を説明

する図である。

【図28】パーソナルコンピュータ1およびロッカーサーバ11による登録の処理を説明するフローチャートである。

【図29】ロッカーサーバ11へのコンテンツの記録の処理を説明するフローチャートである。

【図30】ロッカーサーバ11からのコンテンツの読み出しの処理を説明するフローチャートである。

【図31】本発明に係る音楽データ管理システムの第2の実施の形態を示す図である。

【図32】カメラ付デジタル携帯電話機16を説明する図である。

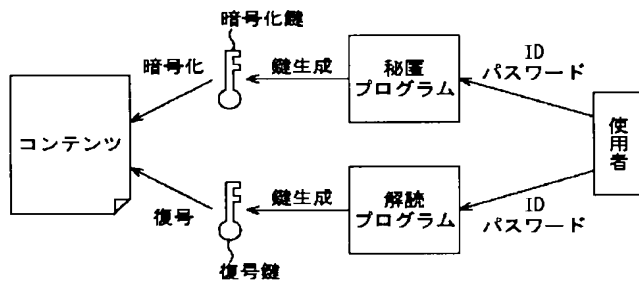
【図33】カメラ付デジタル携帯電話機16を説明する図である。

【図34】カメラ付デジタル携帯電話機16の構成を説明する図である。

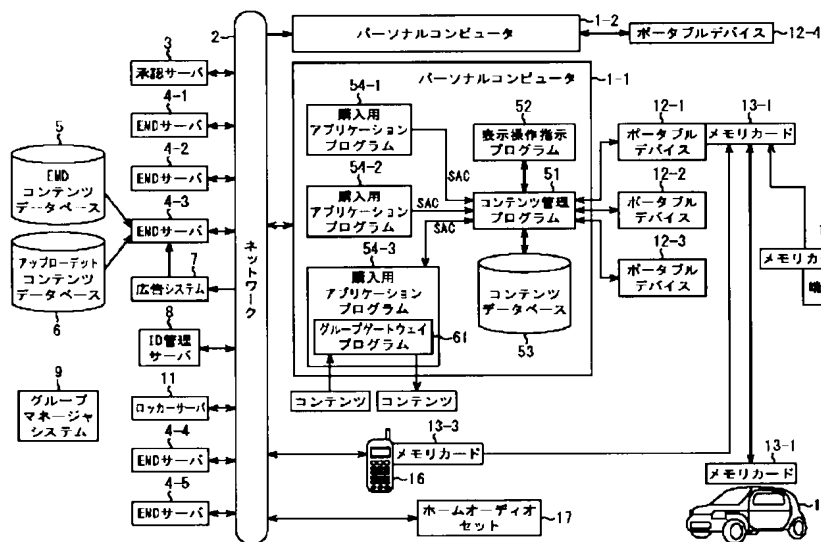
【符号の説明】

1-1, 1-2 パーソナルコンピュータ, 2 ネットワーク, 3 承認サーバ, 8 ID管理サーバ, 11 ロッカーサーバ, 12-1乃至12-4 ポータブルデバイス, 13-1乃至13-3 メモリカード, 16カメラ付デジタル携帯電話機, 51 コンテンツ管理プログラム, 52 表示操作指示プログラム, 53 コンテンツデータベース, 54-1乃至54-3 購入用アプリケーションプログラム, 61 グループゲートウェイプログラム, 71 CPU, 72 ROM, 73 RAM, 81 HDD, 85 通信部, 91 磁気ディスク, 92 光ディスク, 93 光磁気ディスク, 94 半導体メモリ, 101 CPU, 102 ROM, 103 RAM, 111 HDD, 113 通信部, 131 磁気ディスク, 132 光ディスク, 133 光磁気ディスク, 134 半導体メモリ, 401 コンテンツデータベース, 551 主制御部

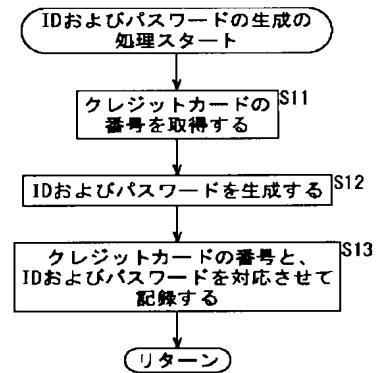
【図1】



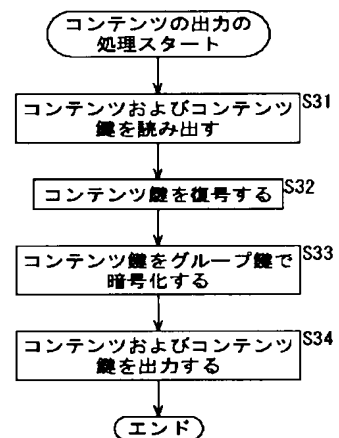
【図2】



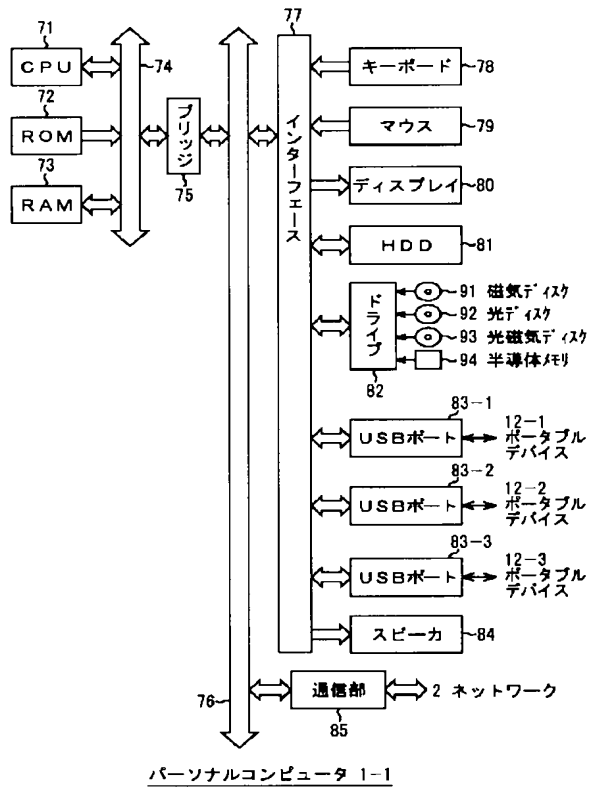
【図13】



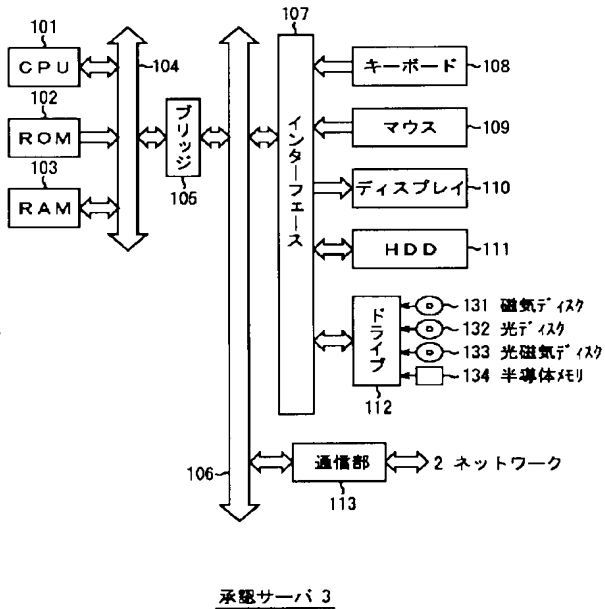
【図14】



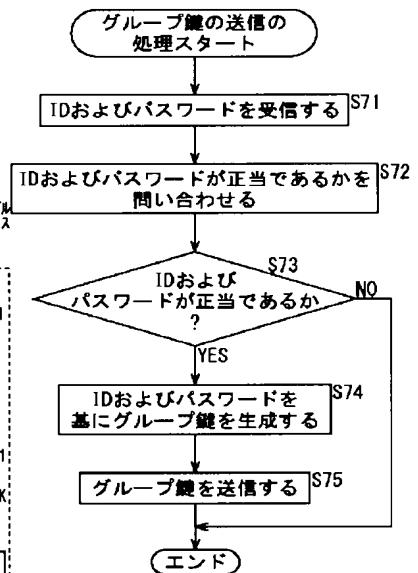
【図 3】



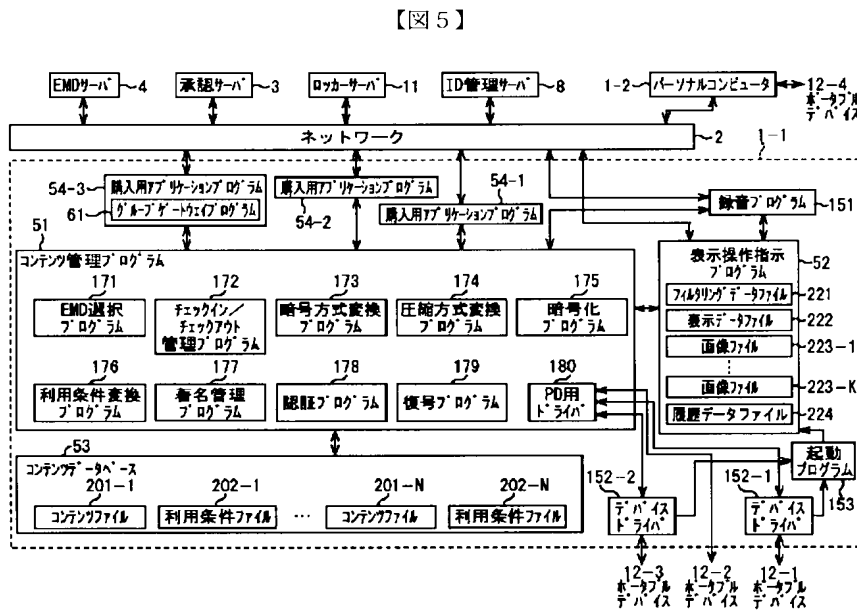
【例 4】



【※ 2 2】

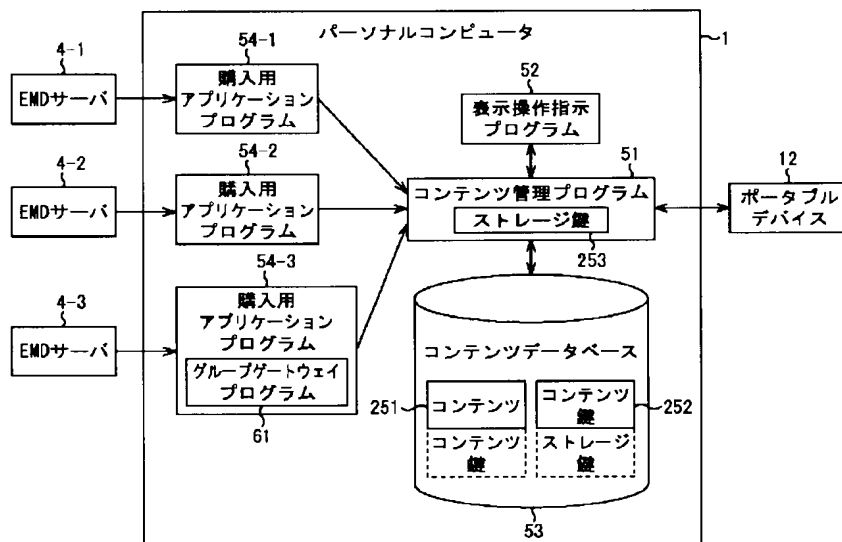


【图 2-4】

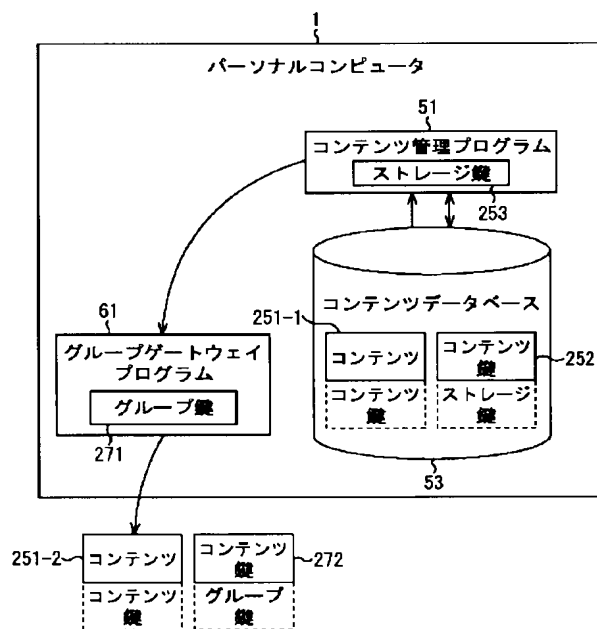


使用者のID	コンテンツ
aaaaa	イイイイイ
bbbbbb	□□□□□
ccccc	ハ\\ハ\\ハ\\ハ
⋮	⋮

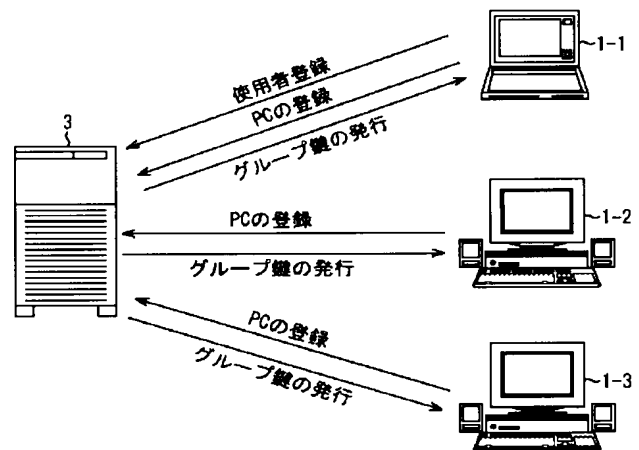
【図6】



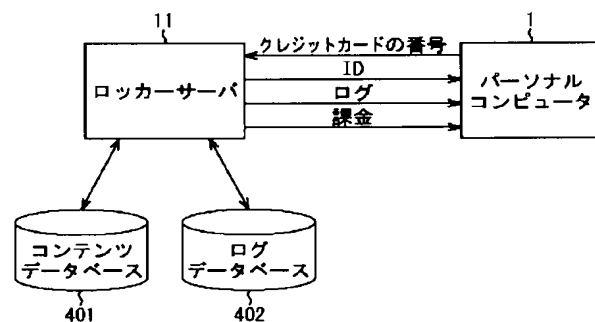
【図7】



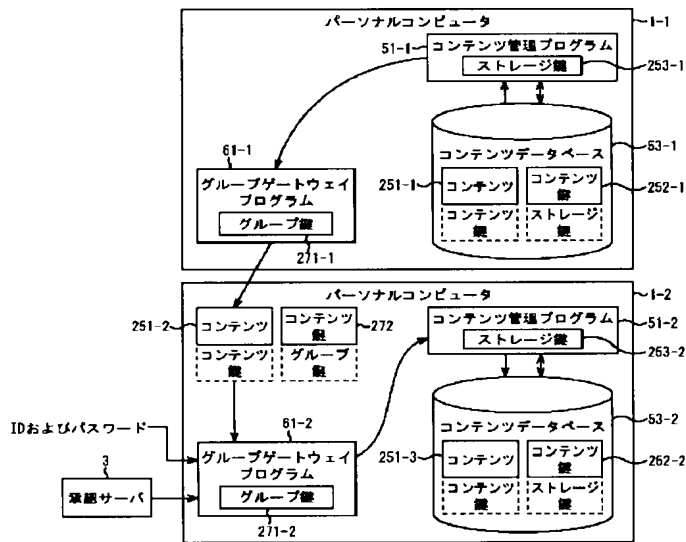
【図10】



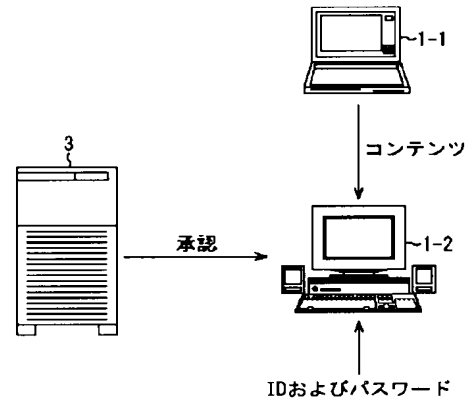
【図23】



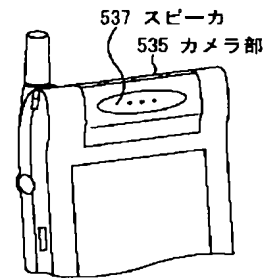
【図8】



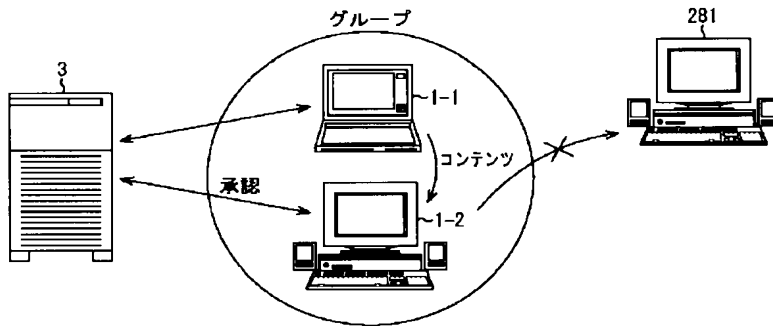
【図11】



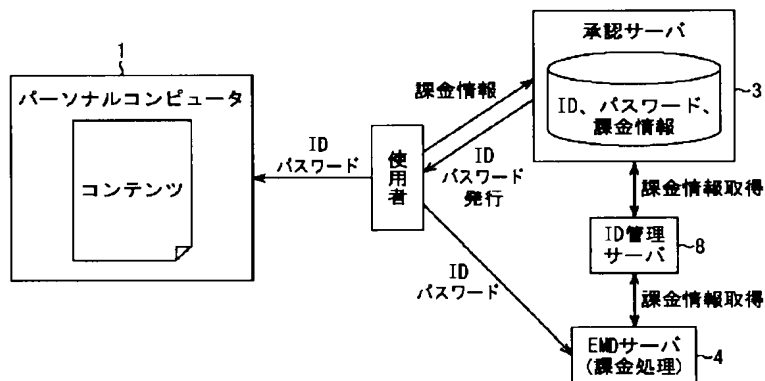
【図33】



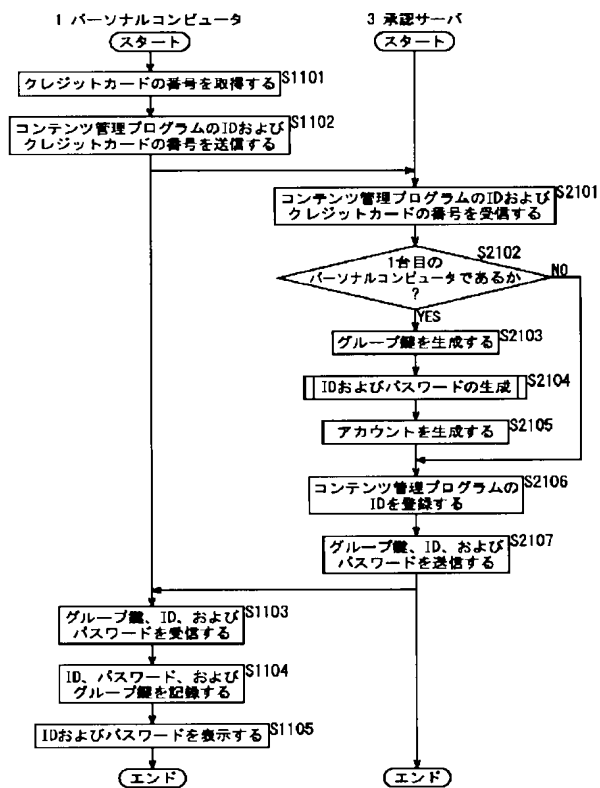
【図9】



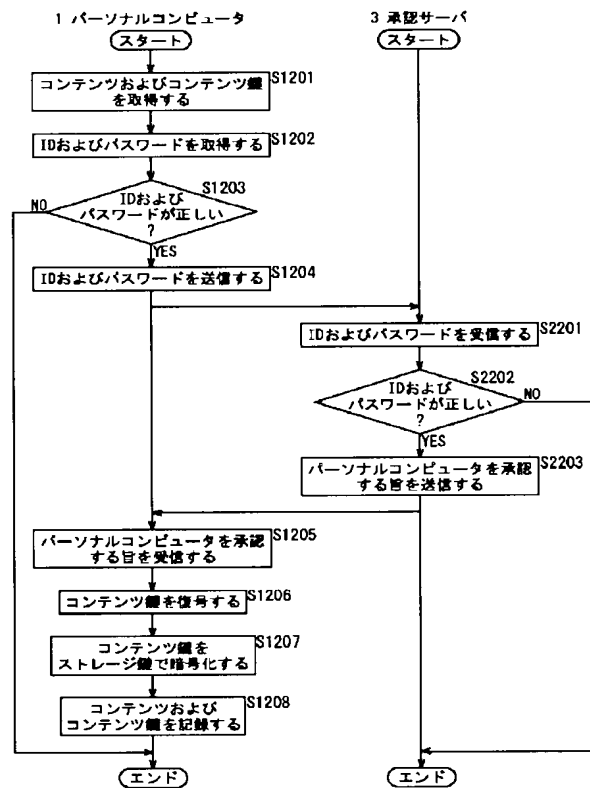
【図16】



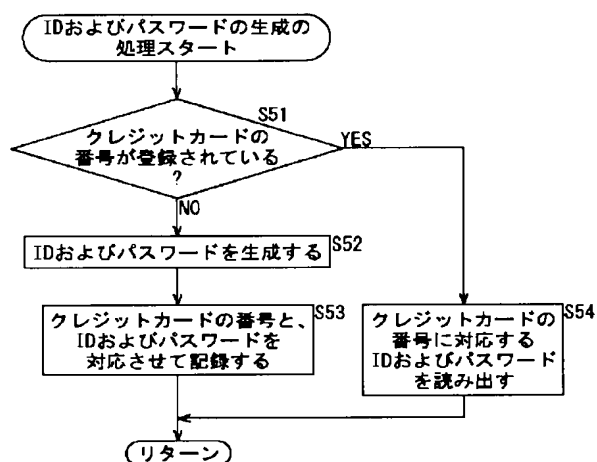
【図12】



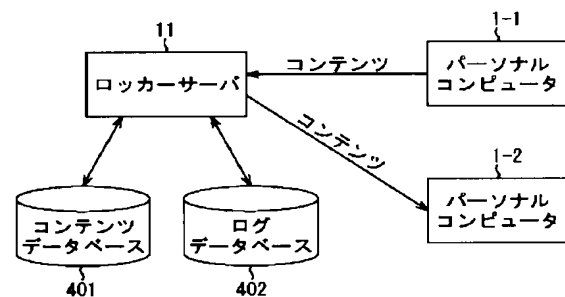
【図15】



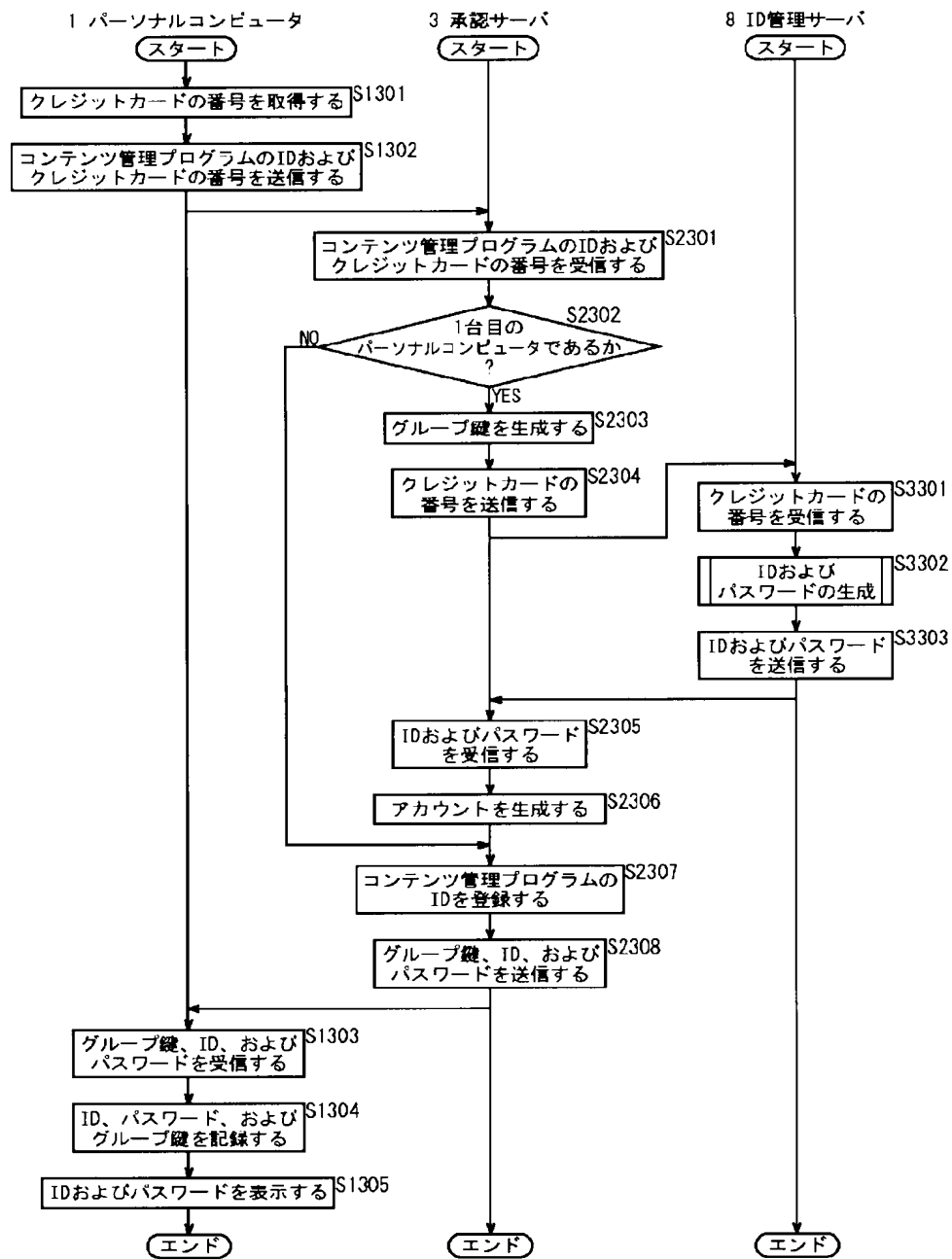
【図18】



【図25】

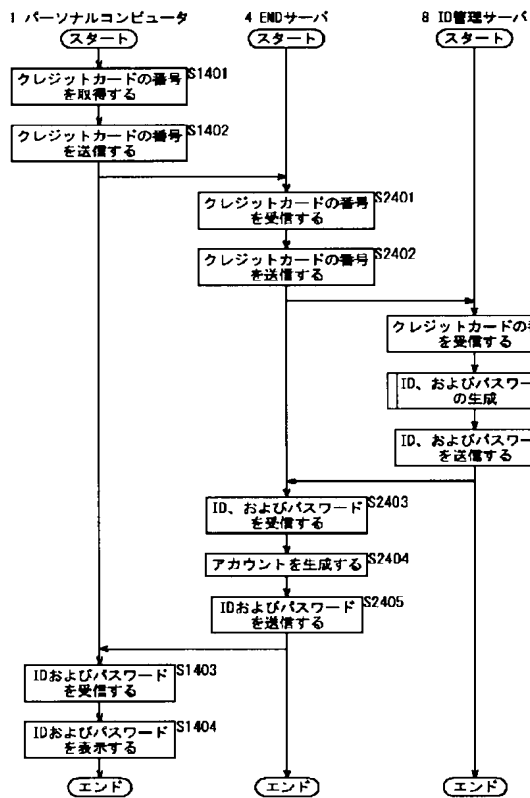


【図17】

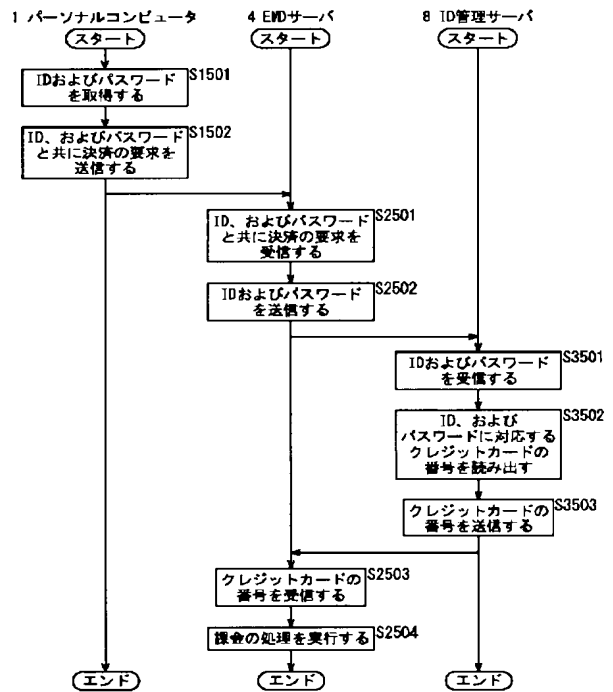




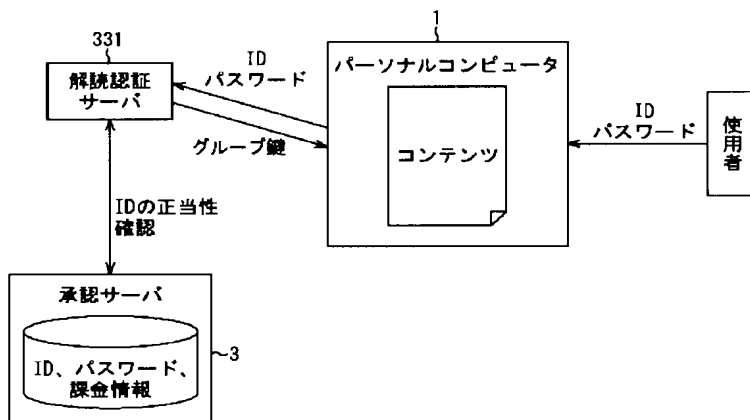
【図19】



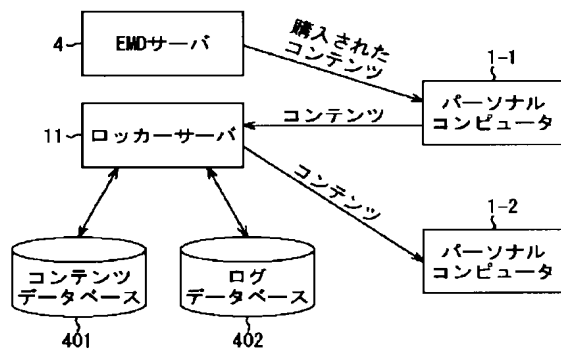
【図20】



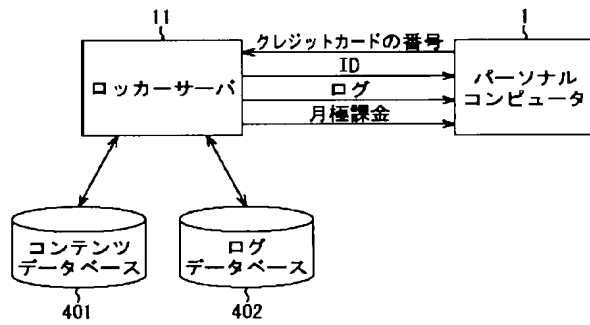
【図21】



【図26】

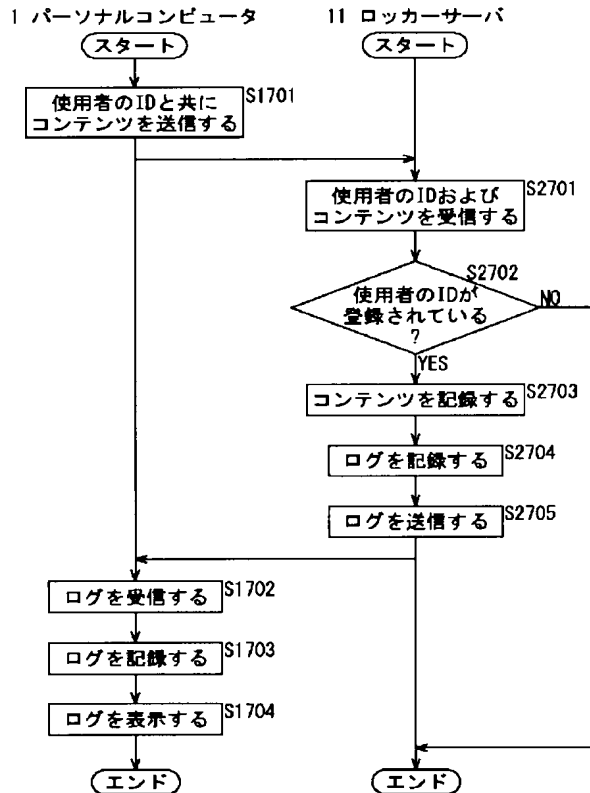
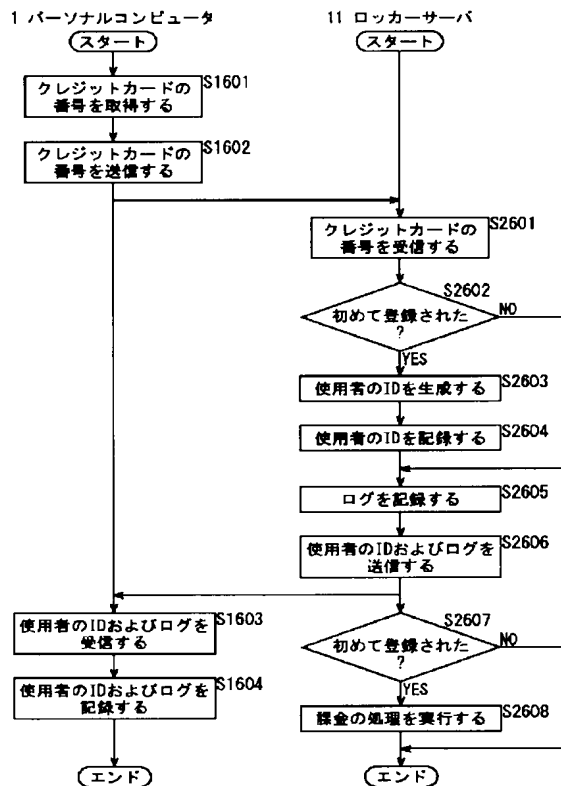


【図27】

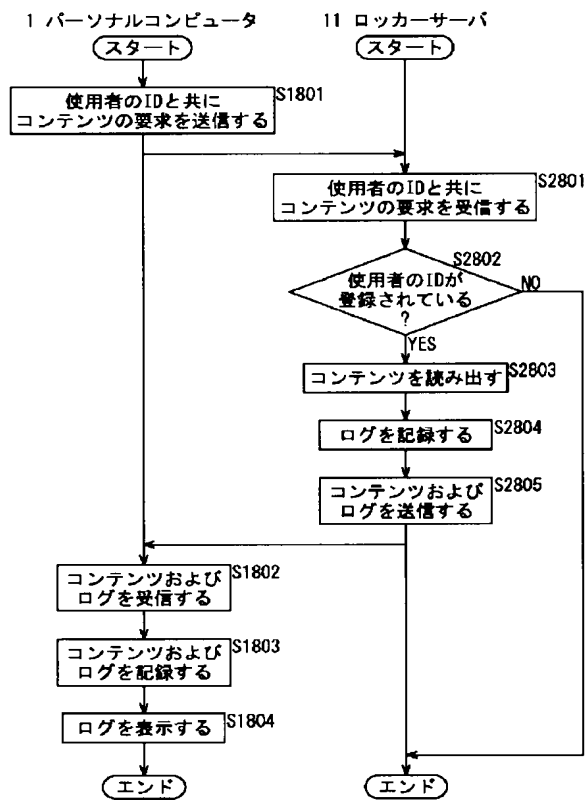


【図29】

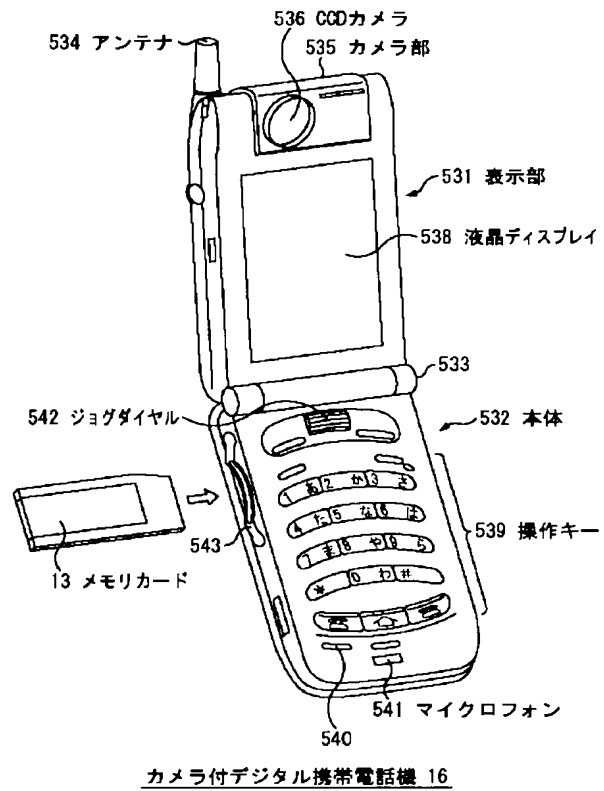
【図28】



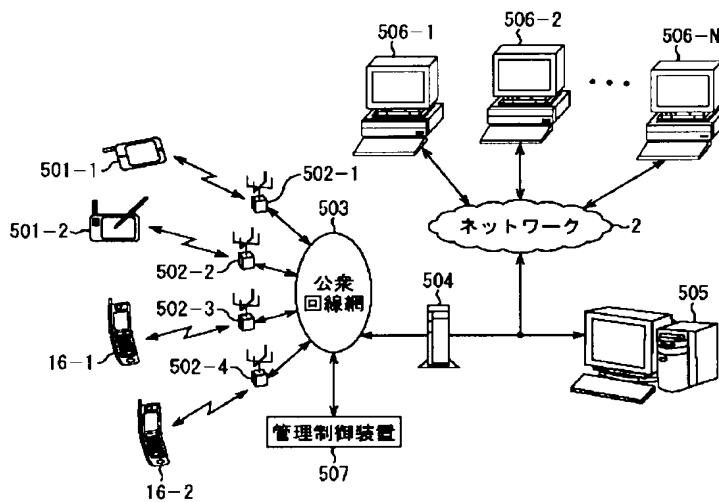
【図30】



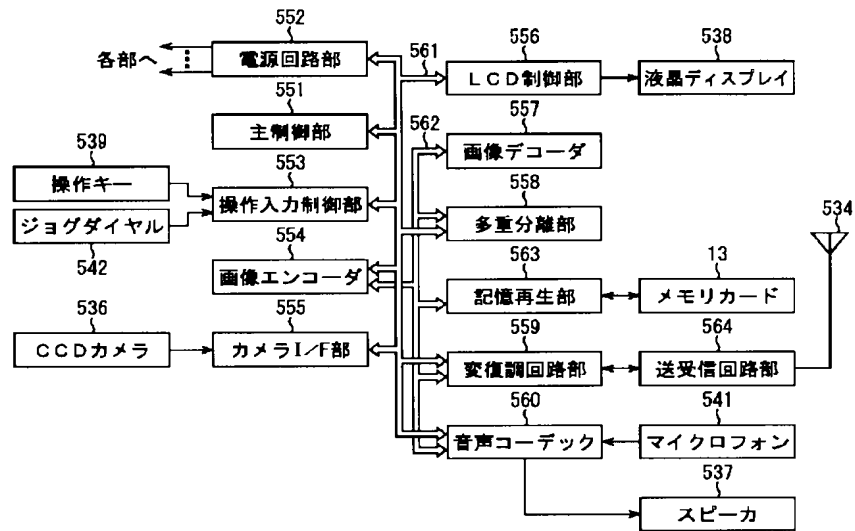
【図32】



【図31】



【図34】



フロントページの続き

(72)発明者 北谷 義道  
東京都品川区北品川6丁目7番35号 ソニ  
ー株式会社内

Fターム(参考) 5B017 AA07 BA05 BA07 CA16  
5J104 AA07 AA13 AA16 EA01 EA06  
EA18 EA26 KA02 KA06 MA02  
NA02 NA05 NA35 PA07 PA11